第 1 章 配置通用功能

在 iSpirit 3626 交换机中，有一些功能很简单，但很常用，一并在本章中介绍，主要包括以下内容：

1、系统基本配置

2、配置文件管理

3、软件版本升级

1.1 系统基本配置

用户可以在全局配置模式（Switch#）下使用 CLI 命令，这些命令用于维护交换机的通常管理，比如修改密码、显示交换机配置信息等。

首先在 EXEC 模式，执行 enable 指令，输入密码后进入全局配置模式，如下所示：

Switch>enable

Password：

Switch#

● 设置交换机的 VLAN1 的 IP 地址及子网掩码

ip address <ip-address><subnet-mask>

例： Switch# ip address 192.168.2.3 255.255.255.0

● 设置交换机的缺省网关

ip gateway <gateway-address>

例：Switch# ip gateway 192.168.2.1

● 重新启动计算机

Switch# reset

● 重新启动计算机，并恢复到出厂模式

Switch# reset factory

● 修改交换机口令，交互式命令，新设的口令需要输入两次

Switch# password

注：交换机缺省 Password 是空

● 把配置信息保存在 flash 中

Switch# save

● 回到上一级模式，如果目前处于全局配置模式，回到 EXEC 模式，如果目前处于 EXEC 模式，执行的命令与 logout 一样。

Switch# exit

● 适用于任何 CLI 模式，退出 TELNET 终端，对串口的终端无效

Switch# logout

● 清除屏幕上的所有信息

Switch# cls

● 测试交换机与远端机器的网络连通性

Switch# ping <remote-host>

例：假设交换机的 IP 地址是 198.168.80.1，有一台直连主机的 IP 地址是 198.168.80.72，交换机测试主机的连通性。

Switch# ping 198.168.80.72

连通显示：

PING 198.168.80.72: 56 data bytes

64 bytes from host (198.168.80.72): icmp_seq=0. time=0. ms

64 bytes from host (198.168.80.72): icmp_seq=1. time=0. ms

64 bytes from host (198.168.80.72): icmp_seq=2. time=0. ms

64 bytes from host (198.168.80.72): icmp_seq=3. time=0. ms

64 bytes from host (198.168.80.72): icmp_seq=4. time=0. ms

—— 198.168.80.72 PING Statistics——

5 packets transmitted, 5 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/3/16

未连通显示：

PING 199.168.80.72: 56 data bytes

no answer from 199.168.80.72

- 显示最近 20 条历史指令

  Switch# show history

- 显示交换机的系统信息。系统描述、产品名称、版本信息、启动时间等

  Switch# show system

- 显示交换机的一些配置信息。IP 地址、MAC、IP gateway 和协议的启用情况

  Switch# show switch

- 显示串口连接参数

  Switch# show console

- 显示当前会话的终端的宽度和高度（能显示多少个字符）

  Switch# show terminal

- 显示交换机的 VLAN1 的 IP 地址信息。IP 地址，子网掩码、网关

  Switch# show ip

- 显示交换机的版本信息

  Switch# version

- 显示交换机的所有 TCP 和 UDP 连接情况

  Switch# show connection

- 清除 TELNET 的登录密码

  Switch# clear telnet password

- 获取系统时间

  Switch# get time

- 配置 CLI 自动退出的时间

Switch# idletime <timeout>

- 显示 CLI 自动退出的时间

Switch# show idletime

- 配置系统时间

Switch# set time

- 配置系统提示符

Switch# switchname <switch-name>

1.2 配置文件管理

当用户修改了交换机的配置后，最好把配置信息存储在 FLASH 中，这样交换机重新启动后配置依然存在。管理员也可以通过 TFTP 完成配置文件的上传和下载。

1.命令

在 CLI 各种模式下都可以执行存储操作：

save

- 在全局配置模式下，可以将交换机的配置文件进行备份，上传到指定的主机上：

upload configuration <ip-address> <name>

ip-address：表示文件上传的目的 PC 的 IP 地址。

name：表示配置文件的命名。

- 在全局配置模式下，可以把指定的主机上的配置文件下载到交换机上：

download configuration <ip-address> <name>

ip-address：表示文件下载的 PC 的 IP 地址。

name：表示下载的文件的文件名。

要想下载的配置能够生效，必须重启交换机。

2.上传和下载配置文件的过程

操作步骤如下：

第一步：搭建备份文件需要网络环境

第二步：将交换机配置信息生成配置文件；

第三步：将配置文件备份到 PC（备份过程已经完成，必要时，进行下一步操作）

第四步：将配置的备份文件重新下载到交换机。

示　例：一台已经配置了 vlan 和接口地址的交换机，需要进行配置文件备份。

第一步：搭建如下所示网络环境

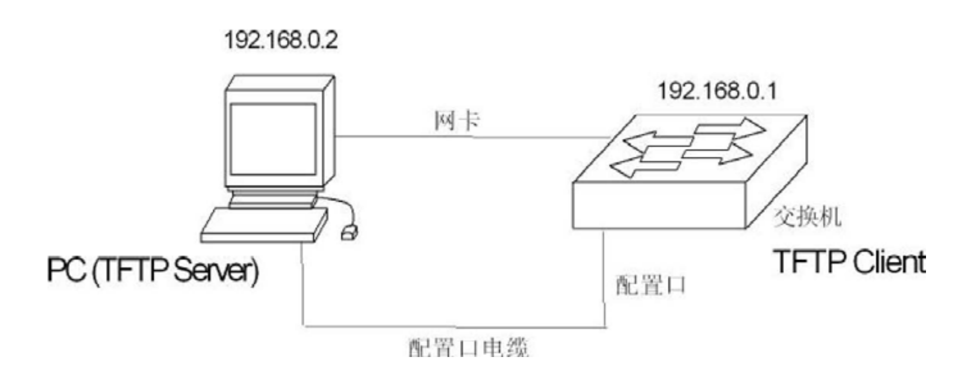


图 1-1 搭建 TFTP 环境

将交换机的配置口通过电缆外接一台配置终端，并通过网线与一台 PC 相连。在 PC 安装 TFTP Server，配置 PC 的以太网口 IP 地址，这里假定 PC 的 IP 地址为 192.168.0.2。然后，配置交换机以太网口 IP 地址，这里假定交换机的 IP 地址为 192.168.0.1。

注意：

PC 网口 IP 地址与交换机以太网口 IP 地址应位于同一网段。

运行 TFTP Server，为备份的配置文件指明路径：

首先，运行 TFTP Server。TFTPD32 窗口界面如下图：

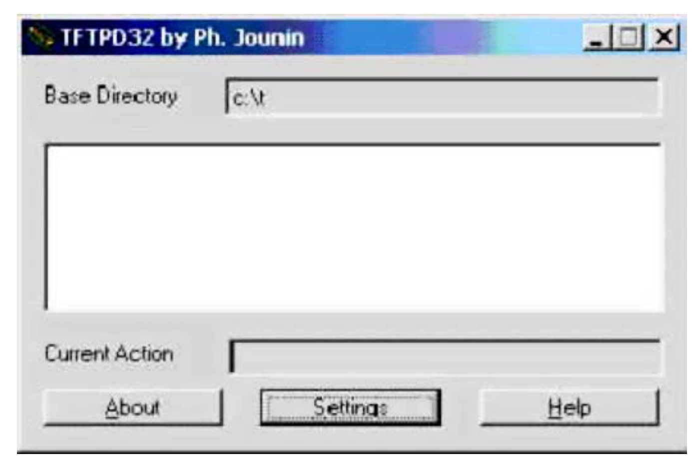


图 1-2 TFTPD32 界面图

然后，设置备份配置文件的目录。具体操作是，单击[Settings]按钮，出现 TFTPD32 设置界面，如下图。

图 1-3 TFTPD32 设置界面图

在“Base Directory”中输入文件路径。单击[OK]按钮确认。

第二步：将交换机的配置信息生成配置文件

在交换机任意管理模式下执行 save 指令，就可以将配置信息生成配置文件。

第三步：将文件备份到 PC 上

Switch# upload configuration 192.168.0.2 beifen

uploading configuration ......

complete

Switch#

第四步：必要时，将备份文件下载到交换机

Switch# download configuration 192.168.0.2 beifen

Do you wish to continue? [Y/N]: y

downloading configuration ......

Complete.

第五步：要想下载的配置文件能够生效，必须重启交换机

Switch# reset

Do you wish to continue？是询问操作是否继续进行。Y 表示是；N 表示否。

1.3 软件版本升级

iSpirit 3626 交换机软件版本支持在线升级。升级是通过工具 TFTP 来完成的。

1.命令

在全局配置模式下，可以将交换机的映像文件升级：

download image <ip-address> <name>

其中<ip-address>为 PC 机的 IP 地址，<file-name>为在 PC 机上映像程序文件名。在下载的过程中不能断电，否则交换机的映像文件可能损坏而造成交换机启动不了。下载完毕后，需要重新启动交换机才能运行新下载的映像文件程序。

2.软件升级过程

升级映像文件步骤：

1、搭建升级环境

第一步：搭建升级环境。如下图所示。

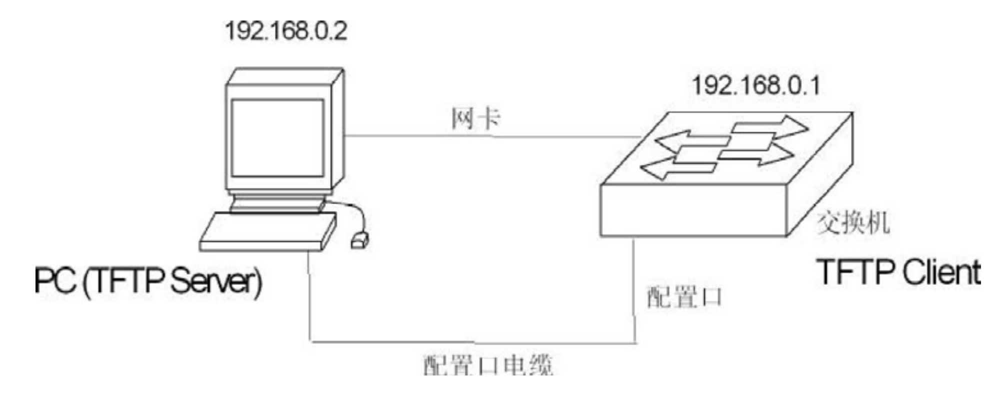


图 1-4 搭建 TFTP 升级环境

第二步：将交换机的配置口通过电缆外接一台配置终端。

第三步：在微机上安装 TFTP Server；

第四步：将新的映像文件拷贝到某一路径下，这里假定路径为 C:\t；

第五步：配置微机的以太网口 IP 地址，这里假定微机的 IP 地址为 192.168.0.2。

第六步：配置交换机以太网口 IP 地址，这里假定交换机的 IP 地址为 192.168.0.1。

注意：

主机网口 IP 地址与交换机以太网口 IP 地址应位于同一网段。

2、运行 TFTP Server

第一步：运行 TFTP Server。TFTPD32 窗口界面如下图：

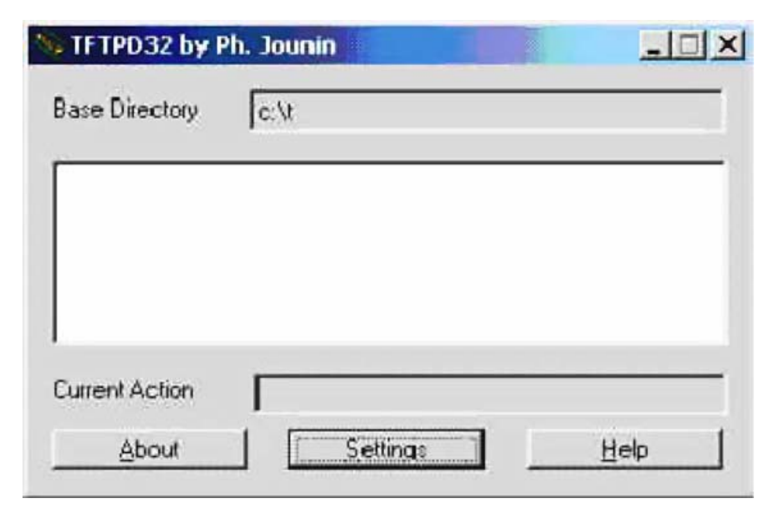


图 1-5　TFTPD32 界面图

第二步：设置 TFTP Server 文件目录。启动 TFTP Server 之后，重新设置 TFTP Server 文件目录，将待加载的

映像文件拷贝到此目录之中。具体操作是，单击[Settings]按钮，出现 TFTPD32 设置界面，如下图。

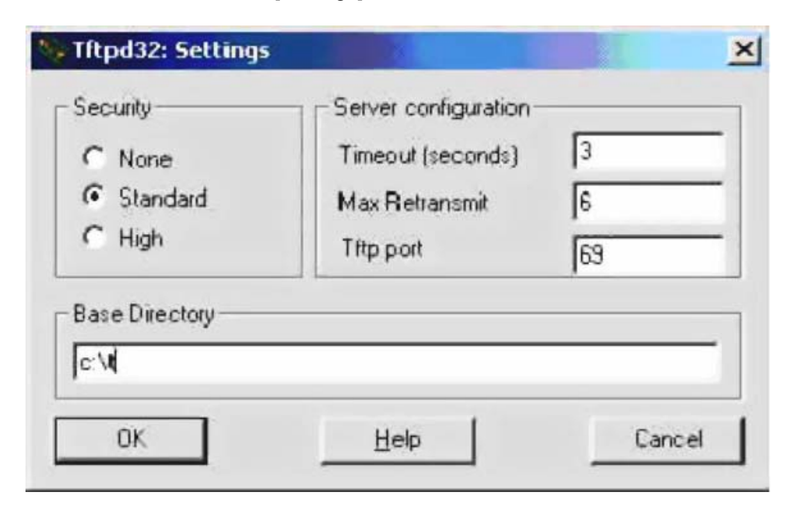


图 1-6　TFTPD32 设置界面图

在“Base Directory”中输入文件路径。单击[OK]按钮确认。

3、配置交换机

第一步：连接交换机，选择以太网接口后，将该接口与运行 TFTP Server 程序的主机通过以太网线连接。并用 ping 命令检测主机与交换机之间是否连通。

第二步：在超级终端 Switch#中输入命令：

Switch# download image 192.168.0.2 lenovo.img，回车，等待下载映像文件完毕。

Do you wish to continue? [Y/N]: y

downloading image......

Complete.

Switch#

注意：交换机升级过程中，不能断电。

第三步：重新启动交换机。

Switch# reset

第 2 章 配置端口

本章对端口相关的配置进行介绍，主要包括以下内容：

1、端口的通用配置

2、配置 MIRROR

3、配置 TRUNK

4、配置 STORM-CONTROL

5、相关配置示例

2.1 端口的通用配置

管理员通过对交换机的端口配置控制端口下接入的用户，如不让端口下的用户接入网络，管理员可以关闭这个端口。本节对端口的通用配置进行介绍，主要包括：

- 端口的打开和关闭
- 端口的速率配置
- 显示端口的信息

1.端口的打开和关闭

iSpirit 3626 交换机的端口缺省是打开的，如果管理员希望端口下的用户不能接入网络，可以关闭这个端口。

- 下面的命令在 PORT RANGE 配置模式下打开一个或多个连续的端口的管理状态：

  enable

  例如打开端口 1 和 2 的管理状态：

  Switch(port 1-2)# enable

- 下面的命令在 PORT RANGE 配置模式下关闭一个或多个连续的端口的管理状态：

  disable

  例如关闭端口 1 和 2 的管理状态：

  Switch(port 1-2)# disable

2.端口的速率配置

- 所有的端口的缺省速率配置是 autonegotiate，对于千兆电口，可以强制成 10M 半双工、10M 全双工、100M 半双工和 100M 全双工。
- 下面的命令在 PORT RANGE 配置模式下配置端口的速率：

  speed <autonegotiate|half-10|full-10|half-100|full-100>

  例如端口 1 和 2 的速率配置成半双工 100M：

  Switch(port 1-2)# speed half-100

3.显示端口的信息

- 下面的命令在全局配置模式或 PORT RANGE 配置模式显示一个或多个连续的端口的信息：

show port <port|port1-port2>

例如显示端口 1 和 2 的信息：

Switch# show port 1-2

2.2 配置 MIRROR

端口镜像对于监听一个或多个端口接收和发送的包的流量是一个非常有用的功能，它能用镜像端口去监听一个或多个端口的接收和发送的包。

联想天工 iSpirit 3626 交换机支持端口镜像功能，镜像端口能够监听别的端口的进入的数据和出去的数据。一个镜像端口可以同时监听多个端口。

本节重点介绍 MIRROR 的配置，主要包括以下内容：

- MIRROR EGRESS
- MIRROR INGRESS
- MIRROR PORT

1.MIRROR EGRESS

这是配置 MIRROR EGRESS 端口，决定监听哪些端口输出的数据包。

2.MIRROR INGRESS

这是配置 MIRROR INGRESS 端口，决定监听哪些端口输入的数据包。

3.MIRROR PORT

这是配置 MIRROR PORT 端口，决定用哪个端口来进行监听，也就是镜像端口。

MIRROR 的配置：mirror 是通过交互式输入配置的。用户根据交互式提示输入配置参数就可以了。

注意：

1.MIRROR EGRESS PORTS 和 MIRRIR INGRESS PORTS 不能包含 MIRROR PORT

2.MIRROR PORT 只能设置一个端口。

2.3 配置 TRUNK

TRUNK 是把多个端口聚合成单个的逻辑端口，它可以用来增加带宽，提供冗余备份连接，还可以用来使得负载均衡。

TRUNK 是很简单的，多个端口被聚合成一个端口来使用，作为目的端口，交换机将会根据软件选择的聚合策略从端口组中某个端口将包发送出去。TRUNK 端口和聚合策略由软件来完成，如果 TRUNK 被用来作冗余备份的话，软件必须检测端口链接情况并且实时的重组 TRUNK.

TRUNK 组里面的所有端口必须是同样的速度，而且是全双工模式才行。TRUNK 是二层的功能，联想天工 iSpirit 3626 交换机支持端口聚合功能。

iSpirit 3626 交换机可支持 32 组 TRUNK,每组 TRUNK 成员最多可达 8 个。需要特别注意的是每一端口只能同时属于一组 TRUNK。

设置 TRUNK 的负载均衡策略，现软件上设置 TRUNK 时 Rtag 的值可设为 1-6，分别对应意义为：

1——非 IP 包基于源 MAC 的均衡策略；

2——非 IP 包基于目的 MAC 的均衡策略；

3——非 IP 包基于源 MAC 和目的 MAC 的均衡策略；

4——IP 包基于源 MAC 以及源 IP 的均衡策略；

5——IP 包基于目的 MAC 以及目的 IP 的均衡策略；

6——IP 包基于源和目的 MAC 以及源和目的 IP 的均衡策略。

本节主要包括以下内容：

- TRUNK 的配置
- TRUNK MCAST 的配置
- TRUNK NO PORTS 的配置
- TRUNK PORTS 的配置
- TRUNK RTAG 的配置
- TRUNK 的显示信息

1.TRUNK 配置

完整的配置一组 TRUNK，先输入 TRUNK 的 ID 号，最大可配置 32 组，接着输入 TRUNK RTAG，有六组均衡策略，最后输入模块/端口号，最多支持 8 个端口聚合。TRUNK 配置是交互式命令如下：

trunk

用户根据交互式提示输入命令参数，要输入的参数是 TRUNK ID，RTAG，TRUNK PORT 列表。

2.TRUNK MCAST 配置

该配置是把已有的一组 TRUNK 加入到已有的组播中去。这里需要特别注意的是该 TRUNK 组的端口集必须是组播端口集的子集才行。具体的是先把 TRUNK 组对应的组播端口从组播端口集中去掉，然后将 TRUNK 组中其中一个端口再重新加入到组播端口中去，默认的是 TRUNK 端口集中端口号最小的那个端口。命令（是一个交互式命令）如下：

trunk mcast

3.TRUNK NO PORTS 配置

该配置是将输入的端口从某个 TRUNK 组端口集中去除。命令如下：

trunk no ports <trunk_id> <port|port1-port2> [port|port1-port2] …

4.TRUNK PORTS 配置

该配置是将输入的端口加入到某个已有的 TRUNK 组端口集中去。命令如下：

trunk ports <trunk_id> <port|port1-port2> [port| port1- port 2] …

5.TRUNK RTAG 配置

该配置是改变已有的某个 TRUNK 组的聚合策略，iSpirit 3626 的 TRUNK 的特点是每组 TRUNK 的均衡策略 RTAG 都可以单独控制。命令如下：

trunk rtag <trunk_id> <rtag>

6.TRUNK 显示信息

在全局 CONFIG 模式下可通过 show trunk 进行 trunk 功能配置的显示。如：

Switch# show trunk

2.4 配置 STORM-CONTROL

在现实生活中，一个 NIC 卡发包时或者很高速率的单播、组播、广播包可以使得网络故障，在这种情况下，交换机上的抑制功能便显得尤为重要，它能防止包涌进阻塞网络的其它部分，联想天工 iSpirit 3626 交换机所有端口支持广播包、组播包和 DLF 包的抑制功能。

iSpirit 3626 交换机实现了针对广播包、组播包和 DLF 单播包的速率进行控制。本节对 STORM-CONTROL 的配置进行详细的描述，主要包括以下内容：

- 缺省配置
- STORM-CONTROL 配置
- 显示 STORM-CONTROL 配置

1.缺省配置

iSpirit 3626 交换机支持对交换机的所有端口设置 broadcast rate, multicast rate, dlf rate。默认端口的广播包抑制到 1500 个，目的是防止网络形成广播风暴。组播和 DLF 包缺省没有做抑制。

2.STORM-CONTROL配置

在 iSpirit 3626 中 STORM-CONFTROL 是统一配置的，storm-control 命令是交互式的输入方式，用户根据提示输入相应的参数。配置后对所有的端口都有效。

3.显示STORM-CONTROL配置

下面的命令在全局配置模式下或者 PORT RANGE 配置模式下显示 STORM-CONTROL 配置：

show storm-control

第 3 章 配置 VLAN

VLAN 是交换机中的一个重要概念，在实际应用中使用非常多，它是内部划分多个网络的基础。VLAN 是虚拟局域网的简称，它是逻辑地把多个设备组织在一起的一个网络，它不管设备的物理位置在哪里。每个 VLAN 都是一个逻辑网络，它具有传统的物理网络的一切功能和属性。每个 VLAN 都是一个广播域，广播包只能在一个 VLAN 内进行广播，不能跨越 VLAN，VLAN 间的数据通信必须通过三层转发。

iSpirit 3626 交换机中有 VLAN 和私有 VLAN 的概念，所以通常又把 VLAN 称为普通 VLAN，本章介绍普通 VLAN 的配置，关于私有 VLAN 的配置请参见“配置私有 VLAN”章节。

本章主要包括以下内容：

1、VLAN 介绍

2、VLAN 配置

3、VLAN 配置示例

3.1 VLAN 介绍

本节对 VLAN 进行一个详细的介绍，主要包括以下内容：

- VLAN 的好处
- VLAN ID
- VLAN 端口成员类型
- VLAN 中继
- 数据流在 VLAN 内的转发
- VLAN 与私有 VLAN 的关系
- VLAN 的子网

1. VLAN的好处

VLAN 极大地扩展了物理网络的规模。传统的物理网络只能有一个很小的规模，最多能容纳上千台设备，而使用 VLAN 划分的物理网络能够容纳上万甚至几十万台设备。VLAN 与传统的物理网络有相同的功能和属性。

使用 VLAN 有以下好处：

VLAN 能有效控制网络中的流量

在传统网络中，不管有无必要，所有的广播包都传送到所有的设备，加重了网络和设备的负载。而 VLAN 能够根据需要把设备组织在一个逻辑网络中，一个 VLAN 就是一个广播域，广播包只在 VLAN 内部传送，不会跨越 VLAN。通过划分 VLAN 可以有效地控制网络中的流量。

VLAN 能够提高网络的安全性

VLAN 内的设备只能与同一个 VLAN 的设备进行二层通信，如果要与另一个 VLAN 通信，必须通过三层转发，如果不建立 VLAN 间的三层转发，VLAN 间完全不能通信，可以起到隔离的作用，保证每个 VLAN 内的数据安全。例如一个公司研发部不想与市场部的数据进行共享，可以研发部建立一个 VLAN，市场部建立一个 VLAN，二个 VLAN 间不建立三层通信通道。

VLAN 使设备的移动变得方便

传统的网络中的设备如果从一个位置移动到另一个位置而属于不同的网络时，需要修改移动设备的网络配置，这样对于用户来说是非常不方便的。而 VLAN 是一个逻辑网络，可以把不在同一物理位置的设备划在同一个网络，当设备移动时还可以使设备属于此 VLAN 中，这样移动的设备不需要修改任何配置。

2. VLAN ID

每一个 VLAN 有一个标识号，叫 VLAN ID，VLAN ID 的范围从 0 到 4095，其中 0 和 4095 不用，实际有效的只有 1 到 4094。VLAN ID 唯一标识一个 VLAN。

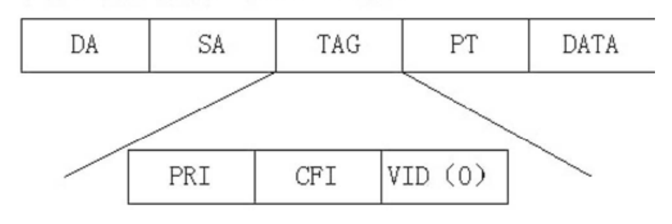
iSpirit 3626 交换机支持 255 个 VLAN，在创建 VLAN 时，要选择一个 VLAN ID，范围从 1 到 4094。

在网络中的一个 VLAN 内传输的数据帧有三种：不带标记的数据帧，带 VID 为 0 的标记的数据帧，带 VID 非 0 的标记的数据帧。如下图所示为三种不同数据帧格式。

不带标记的数据帧

DA	SA	PT	DATA

带标记的数据帧，但VLAN ID为0



带标记的数据帧，但VLAN ID非0

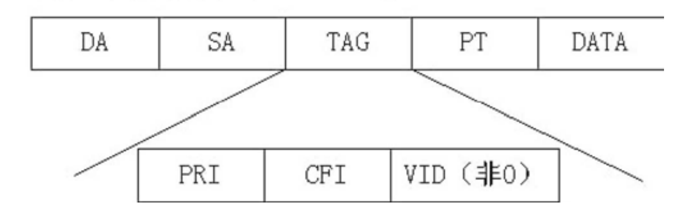


图 3-1　三种不同的数据帧格式

在交换机内部所有的数据帧都是带标记的。如果一个不带标记的数据帧输入交换机，交换机要给该数据帧加上一个标记，选择一个 VLAN ID 值填入标记的 VID 中。如果一个带 VID 为 0 的标记的数据帧输入交换机，交换机选择一个 VLAN ID 值填入标记的 VID 中。如果一个带 VID 非 0 的标记的数据帧输入交换机，该帧不变。

3. VLAN端口成员类型

iSpirit 3626 交换机支持基于端口的 VLAN 和基于 802.1Q 的 VLAN。一个 VLAN 包括两种端口成员类型：untagged 成员和 tagged 成员。一个 VLAN 可以既包括 untagged 端口成员，又包括 tagged 端口成员。

一个 VLAN 可以没有端口成员，也可以有一个或多个端口成员。当一个端口属于一个 VLAN 时，可以是 VLAN 的

untagged 成员或 tagged 成员。

一个端口最多只能属于一个 VLAN 的 untagged 成员，当一个端口设置成一个 VLAN 的 untagged 成员时，如果该端口还属于其它 VLAN 的 untagged 成员，则把该端口从其它 VLAN 中清除，也就是端口最后设置的生效。

一个端口可以属一个或多个 VLAN 的 tagged 成员，如果一个端口属于两个或多个 VLAN 的 tagged 成员时，这个端口又称为 VLAN 中继端口。一个端口可以同时属于一个 VLAN 的 untagged 成员和属于另外的一个或多个 VLAN 的 tagged 成员。

4. VLAN中继

如果一个端口属于两个或多个 VLAN 的 tagged 成员，那么这个端口又称为 VLAN 中继端口。两个交换机之间可以以 VLAN 中继端口相连，这样两个交换机之间可以划分两个或多个共同的 VLAN。

如图 3-2 是一个 VLAN 中继的例子，两个交换机之间以 VLAN 中继端口相连，是 VLAN 2 和 VLAN 3 的中继端口，每个交换机划分为两个 VLAN，分别是 VLAN 2 和 VLAN 3，每个 VLAN 内有一个用户。这样，用户 1 可以与用户 3 通信，用户 2 可以与用户 4 通信，用户 1 和用户 3 不能与用户 2 和用户 4 通信。

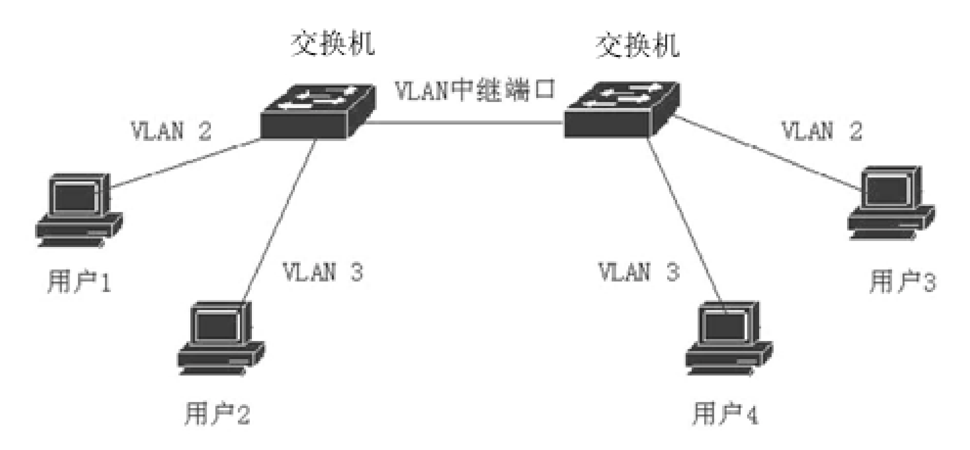


图 3-2　VLAN 中继端口

5.数据流在VLAN内的转发

当交换机从一个端口收到一个数据包时，根据以下步骤进行二层转发：

1) 决定该数据包所属的 VLAN。
2) 判断该数据包是广播数据包、组播数据包还是单播数据包。
3) 根据不同的数据包确定输出端口（可以是零个、一个或多个输出端口），如果没有输出端口，丢弃该数据包。
4) 根据输出端口在 VLAN 内的成员类型决定发出去的包是否带标记。
5) 从输出端口发送出去。

● 如何决定数据包的所属 VLAN：

如果收到的数据包带标记并且标记中的 VID 字段非 0 时，该数据包所属的 VLAN 就是标记中 VID 值。

如果收到的数据包不带标记或带标记但标记中的 VID 值为 0 时，如果输入端口是某个 VLAN 的 untagged 成员，则该 VLAN 是该数据包所属的 VLAN，如果输入端口不是任何 VLAN 的 untagged 成员，则丢弃该数据包。

● 如何确定数据包的类型：

如果收到的数据包的目的 MAC 地址是 FF:FF:FF:FF:FF:FF，则该数据包是广播数据包。

如果收到的数据包不是广播数据包且其目的 MAC 地址的第 40 位为 1，则该数据包是组播数据包。

如果既不是广播数据包又不是组播数据包，则该数据包为单播数据包。

● 如何决定数据包的输出端口：

如果输入的数据包是广播数据包，该数据包所属的 VLAN 的所有成员端口就是数据包的输出端口。

如果输入的数据包是组播数据包，首先根据目的组播 MAC 地址和所属的 VLAN 查找二层硬件组播转发表，如果找到匹配的组播条目，则组播条目中的输出端口和所属 VLAN 中的成员端口中的共同端口（与操作）为数据包的输出端口，如果没有共同的端口，该数据包丢弃。如果在二层硬件组播转发表中没有找到匹配的组播条目，根据二层硬件组播转发表的转发模式决定输出端口，如果是未注册组播转发模式，组播包当作广播处理，所属的 VLAN 的所有成员端口就是数据包的输出端口，如果是注册转发模式，则没有输出端口，数据包丢弃。

如果输入的数据包是单播数据包，首先根据目的 MAC 地址和所属的 VLAN 查找二层硬件转发表，如果找到匹配的条目，则条目中的输出端口与所属 VLAN 的成员端口中的共同端口（与操作）为数据包的输出端口，如果没有共同的端口，该数据包丢弃。如果在二层硬件转发表中没有找到匹配的条目，该数据包当作广播包处理，所属的 VLAN 的所有成员端口就是数据包的输出端口。

● 发送数据包：

决定了输入的数据包的输出端口后要把数据包从所有的输出端口发送出去。

如果某个输出端口是数据包所属的 VLAN 的 untagged 成员，则数据包从该输出端口发送出去时不带标记。

如果某个输出端口是数据包所属的 VLAN 的 tagged 成员，则数据包从该输出端口发送出去时带标记，标记中的 VID 值是数据包所属的 VLAN 的值。

6. VLAN与私有VLAN的关系

因为 iSpirit 3626 上实现了私有 VLAN，所以 VLAN 有称为普通 VLAN。普通 VLAN 和私有 VLAN 之间存在着一定的互斥的关系。

普通 VLAN 中的一个 VLAN 就是一个广播域，每个 VLAN 可以创建一个子网，VLAN 间通信必须通过三层转发。而私有 VLAN 中一个私有 VLAN 组才是一个广播域，每个私有 VLAN 组可以创建一个子网，在私有 VLAN 组的主 VLAN 之上创建子网，私有 VLAN 组间通信必须通过三层转发，而私有 VLAN 组内通信则是二层转发。

在创建普通 VLAN 时，要保证该 VLAN 不在任何私有 VLAN 组中的 VLAN 范围内，如果该 VLAN 在私有 VLAN 组的 VLAN 范围内，则创建不成功。

如果私有 VLAN 组中要设置的混杂端口、共用端口或隔离端口是某个普通 VLAN 的 untagged 成员，则要从该普通 VLAN 中清除该端口，即该端口不再属于该普通 VLAN 的 untagged 成员。

在设置普通 VLAN 的端口成员时，如果一个端口被私有 VLAN 组占用，则该端口不能设置成该 VLAN 的 untagged 成员，但是该端口可以设置成该 VLAN 的 tagged 成员。

在使用命令 show vlan 显示 VLAN 的信息时，只能显示普通 VLAN 的信息，不能显示私有 VLAN 的信息，需要使用 show privatevlan 显示私有 VLAN 的信息。

7. VLAN的子网

在 iSpirit 3626 交换机上一个 VLAN 是一个广播域，一个 VLAN 上可以建立一个子网接口，所有的子网都是建立在 VLAN 的基础上的。iSpirit 3626 交换机上最多可划分 4094 个 VLAN，但最多只能建立 26 个子网，当在 26 个 VLAN 上建立了子网后，其它的 VLAN 就不能建立子网接口。

3.2 VLAN 配置

为了使用户能够更加方便地配置 VLAN 功能，iSpirit 3626 交换机提供了多样化的命令，这些命令主要在 VLAN 配置模式和 PORT RANGE 配置模式之下。

iSpirit 3626 交换机缺省情况下有一个 VLAN 1，所有的端口是 VLAN 1 的 untagged 成员。

本节对 VLAN 的配置进行详细的介绍，主要包括以下内容：

- 创建和删除 VLAN
- 配置 VLAN 的 untagged 成员
- 配置 VLAN 的 tagged 成员
- 显示 VLAN 的信息

1.创建和删除VLAN

iSpirit 3626 交换机可以一次创建一个或多个连续的 VLAN。下面的命令在全局 CONFIG 模式下创建 VLAN。如果输入 vlanid，此时只创建一个 VLAN，并进入 VLAN 配置模式，如果该 VLAN 已经存在了，则不创建，只进入 VLAN 配置模式。如果输入 minvlanid-maxvlanid，则创建多个连续的 VLAN，此时不进入 VLAN 配置模式，如果 minvlanid-maxvlanid 范围内的 VLAN 存在，则该 VLAN 不进行创建操作：

vlan {<vlanid> | <minvlanid-maxvlanid>}

iSpirit 3626 交换机可以一次删除一个或多个连续的 VLAN。下面的命令在全局 CONFIG 模式下删除 VLAN。如果输入 vlanid，此时只删除一个 VLAN，如果该 VLAN 不存在，不进行删除操作。如果输入 minvlanid-maxvlanid，此时删除多个连续的 VLAN，如果在 minvlanid-maxvlanid 范围内的 VLAN 不存在，则该 VLAN 不进行删除操作。如果一个 VLAN 被删除，该 VLAN 内的成员关系全部消失：

no vlan {<vlanid> | <minvlanid-maxvlanid>}

注意：

如果一个 VLAN 已经被私有 VLAN 占用，则该 VLAN 不能被创建和删除。

2.配置VLAN的untagged成员

iSpirit 3626 交换机支持在 VLAN 配置模式和 PORT RANGE 配置模式下设置 VLAN 的 untagged 成员端口。

- 下面的命令在 VLAN 配置模式下增加 VLAN 的 untagged 成员端口：

  untagged {<port>|<port1-port2>} [<port>|<port1-port2>] …

- 下面的命令在 VLAN 配置模式下删除 VLAN 的 untagged 成员端口：

  no untagged {< port >|< port 1- port 2>} [<port >|< port 1- port 2>] …

- 下面的命令在 PORT RANGE 配置模式下把一个或多个连续的端口加到 VLAN 中去，属于 VLAN 的 untagged 成员：

  untagged-vlan <vlanid>

● 下面的命令在 PORT RANGE 配置模式下把一个或多个连续的端口从 VLAN 中清除：

no untagged-vlan <vlanid>

注意：

如果一个端口已经被私有 VLAN 占用，则该端口不能成为 VLAN 的 untagged 成员。

如果一个端口已经属于一个 VLAN 的 untagged 成员，则要从该 VLAN 中清除该端口，该端口不再属于该 VLAN 的成员。

3.配置VLAN的tagged成员

iSpirit 3626 交换机支持在 VLAN 配置模式和 PORT RANGE 配置模式下设置一个或多个 VLAN 的 tagged 成员端口。

● 下面的命令在 VLAN 配置模式下增加 VLAN 的 tagged 成员端口：

tagged {< port >|< port 1- port 2>} [<port >|< port 1- port 2>] …

● 下面的命令在 VLAN 配置模式下删除 VLAN 的 tagged 成员端口：

no tagged {< port >|< port 1- port 2>} [<port >|< port 1- port 2>] …

● 下面的命令在 PORT RANGE 配置模式下把一个或多个连续的端口加到一个或多个 VLAN 中去，属于 VLAN 的 tagged 成员：

tagged-vlan{<vlanid>|<minvlanid-maxvlanid>} [<vlanid>|<minvlanid-maxvlanid>] …

● 下面的命令在 PORT RANGE 配置模式下把一个或多个连续的端口从一个或多个 VLAN 中清除：

no tagged-vlan {<vlanid>|<minvlanid-maxvlanid>} [<vlanid>|<minvlanid-maxvlanid>] …

4.显示VLAN的信息

iSpirit 3626 交换机支持在多个模式下显示 VLAN 的信息，包括 VLAN 的总体信息和 VLAN 内的端口成员信息。

● 下面的命令显示 VLAN 的信息，如果没有输入任何参数，则列出所有的 VLAN 的总体信息，如果有输入参数，则显示一个或多个 VLAN 的端口成员信息：

show vlan [<vlanid>|<minvlanid-maxvlanid>] …

第 4 章 配置私有 VLAN

在实际的应用中，为了保证公用数据的共享和私有数据的安全，二层的端口隔离技术使用得非常多。为了能够让用户使用端口隔离技术并且能够更加简便地配置端口隔离，联想网络推出了私有 VLAN 的概念并在 iSpirit 3626 交换机上实现。

私有 VLAN 由多个连续的 VLAN（VLAN ID 是连续的）组成，通过端口的划分，在一个广播域中实现二层的端口隔离。使用私有 VLAN 技术，只需要掌握私有 VLAN 的几个概念，配置端口隔离就非常简单。

本章对私有 VLAN 技术及配置进行详细的描述，主要包括以下内容：

1、私有 VLAN 介绍

2、私有 VLAN 配置

3、私有 VLAN 配置示例

4.1 私有 VLAN 介绍

iSpirit 3626 交换机实现了 12 组私有 VLAN，每一组私有 VLAN 是一个广播域，也就是说一组私有 VLAN 只能创建一个子网，内部由多个连续的 VLAN 组成，实现内部的端口隔离。私有 VLAN 组间是不同的广播域，也就是说是不同的子网网段，私有 VLAN 组间必须通过三层转发通信。

本节对私有 VLAN 进行一个详细的描述，主要包括以下内容：

- 私有 VLAN 的端口类型
- 私有 VLAN 的 VLAN 范围
- 私有 VLAN 和普通 VLAN 的关系
- 私有 VLAN 的子网

1.私有VLAN的端口类型

私有 VLAN 有三种类型的端口：混杂端口、共用端口和隔离端口。混杂端口是私有 VLAN 组中的上连端口，而共用端口和隔离端口是被隔离的对象。

混杂端口是私有 VLAN 组中的上连端口，一个私有 VLAN 组中有一个或多个混杂端口，而且一个私有 VLAN 组中必须要有至少一个混杂端口。混杂端口可以与该私有 VLAN 组的任何端口（包括混杂端口、共用端口和隔离端口）进行二层通信。在实际应用中，一般公用的数据服务器和互联网的出口与混杂端口相连。

共用端口是私有 VLAN 组中被隔离的对象。共用端口有组的概念，一个或多个共用端口组成一个共用端口组，iSpirit 3626 交换机中的一个私有 VLAN 组最多支持 6 个共用端口组。共用端口能够与混杂端口和共用端口组内的其它共用端口通信，共用端口不能与隔离端口和其它共用端口组中的端口通信。如果一个共用端口组中只有一个端口，该共用端口组实质就是一个隔离端口。

隔离端口是私有 VLAN 组中被隔离的对象，隔离端口没有组的概念，隔离端口之间都是互相隔离的。隔离端口只能与混杂端口通信，不能与其它隔离端口和共用端口通信。

一个私有 VLAN 中必须要有被隔离的对象，一个私有 VLAN 组中必须至少要有一个隔离端口或一个共用端口组。一个私有 VLAN 组中可以没有隔离端口，但此时一定有一个或多个共用端口组。一个私有 VLAN 组中可以没有共用端口组，但此时一定有一个或多个隔离端口。如果一个私有 VLAN 组中只有一个隔离端口或一个共用端口组，实际上也



起不到隔离的效果，因此在实际应用中，一个私有 VLAN 组中至少有两个被隔离的对象。

私有 VLAN 组内的端口不能重叠，也就是说一个端口只能是隔离端口、共用端口和混杂端口中的一种，如果一个端口是共用端口，不能与共用端口组内的其它端口或其它共用端口组的端口相同。私有 VLAN 组间的端口不能重叠，也就是说一个端口只能属于一个私有 VLAN 组。

如图 4-1 所示是一个私有 VLAN 组的例子，端口 1-6 和 10-12 属于一个私有 VLAN 组，端口 1 和端口 2 是隔离端口，端口 3、4、5 和 6 是共用端口，其中端口 3 和 4 是一个共用端口组，端口 5 和 6 是一个共用端口组，端口 10、11 和 12 是混杂端口。用户 1 和用户 2 只能访问服务器 1、服务器 2 和互联网，用户 1 和用户 2 之间不能通信，用户 1 和用户 2 不能与用户 3 到 6 通信。用户 3 和用户 4 可以访问服务器 1、服务器 2 和互联网，用户 3 和用户 4 之间可以通信，用户 3 和用户 4 不能与用户 1 到 2、用户 5 到 6 通信。用户 5 和用户 6 可以访问服务器 1、服务器 2 和互联网，用户 5 和用户 6 之间可以通信，用户 5 和用户 6 不能与用户 1 到 4 通信。服务器 1 和服务器 2 可以和用户 1 到 6 通信，可以访问互联网，服务器 1 和服务器 2 之间可以通信。

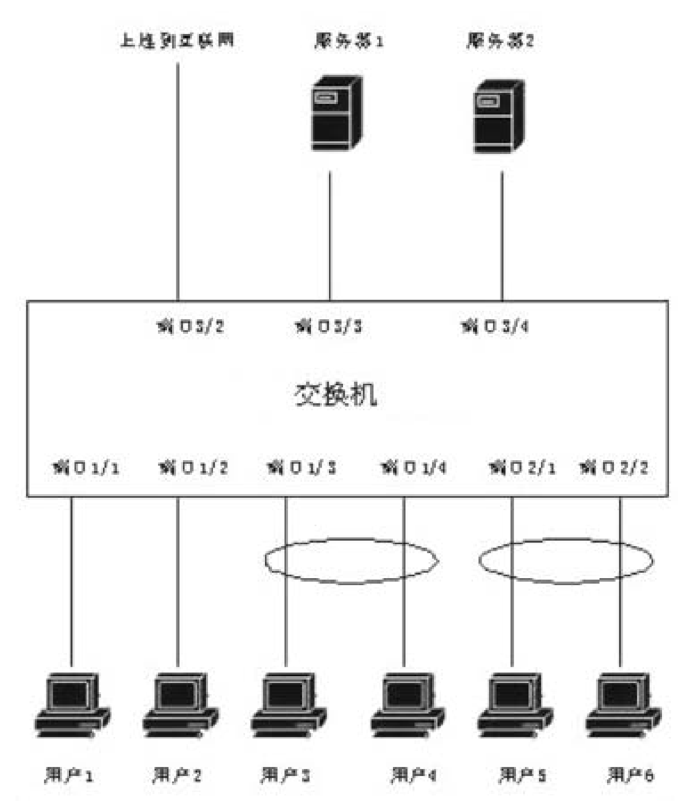


图 4-1　一个私有 VLAN 组

如图 4-2 所示是两个私有 VLAN 组的例子，私有 VLAN 组 1 包括端口 1-3 和端口 11，私有 VLAN 组 2 包括端口 5-7 和端口 12。在私有 VLAN 组 1 中，端口 1 是隔离端口，端口 2 和 3 是共用端口，端口 2 和 3 组成一个共用端口组，端口 11 是混杂端口。在私有 VLAN 组 2 中，端口 5 是隔离端口，端口 6 和 7 是共用端口，端口 6 和 7 组成一个共用端口组，端口 12 是混杂端口。在私有 VLAN 组 1 中，用户 1 只能与服务器 1 通信，用户 1 不能与用户 2 到 3 通信，用户 2 和用户 3 可以与服务器 1 通信，并且用户 2 和用户 3 能够互相通信，但不能与用户 1 通信。在私有 VLAN 组 2 中，用户 4 只能与服务器 2 通信，用户 4 不能与用户 5 到 6 通信，用户 5 和用户 6 可以与服务器 2 通信，并且用户 5 和用户 6 能够互相通信，但不能与用户 4 通信。私有 VLAN 组 1 中的设备要和私有 VLAN 组 2 中的设备通信必须要通

过三层转发。

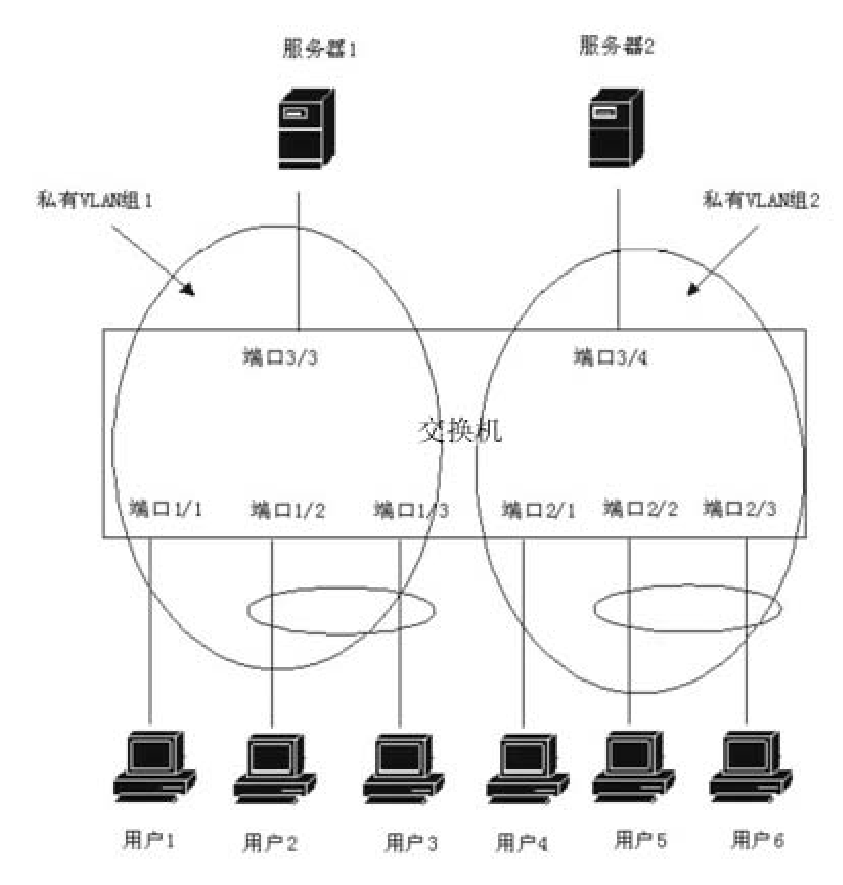


图 4-2　两个私有 VLAN 组

2.私有VLAN的VLAN范围

一个私有 VLAN 组是由连续的多个 VLAN 组成。在建立一个私有 VLAN 组时，需要选择 VLAN ID 是连续的多个 VLAN，私有 VLAN 组中的多个 VLAN 共享一个广播域，属于同一个子网，私有 VLAN 组间的通信必须通过三层转发。私有 VLAN 组间的 VLAN 不能重叠， 例如一个私有 VLAN 组选择 VLAN 10 到 19 作为该组内的 VLAN，那另一个私有 VLAN 组的 VLAN 范围不能包括 VLAN 10 到 19 的任何一个。

每一个私有 VLAN 组都有唯一的一个主 VLAN，主 VLAN 必须在私有 VLAN 组内的 VLAN 范围内，可以从此 VLAN 范围内任意选择一个 VLAN 作为主 VLAN。例如一个私有 VLAN 组选择 VLAN 10 到 19 作为该组内的 VLAN，那么可以选择 VLAN 10 到 19 中的任意一个作为主 VLAN。主 VLAN 的用处是为了创建私有 VLAN 组的子网，因为一个私有 VLAN 组只能有一个子网，所以直接在主 VLAN 上创建私有 VLAN 组的子网，私有 VLAN 组内的其它 VLAN 不能创建子网。

在选择私有 VLAN 组内的 VLAN 范围时，VLAN 范围要足够大，否则私有 VLAN 组最后不能生效。私有 VLAN 组内的 VLAN 范围是由隔离端口和共用端口组的个数决定的，一个隔离端口要占用一个 VLAN，一个共用端口组要占用一个 VLAN。可以得到私有 VLAN 组内的 VLAN 范围的一个等式：（私有 VLAN 组内的 VLAN 个数 >= 私有 VLAN 组内的隔离端口个数+ 私有 VLAN 组内的共用端口组个数 + 1）例如图 1，私有 VLAN 组内的隔离端口个数是 2 个，共

用端口组个数是 2 个，所以私有 VLAN 组内的 VLAN 个数最少要 5（2+2+1）个。

私有 VLAN 组内的 VLAN 个数有一个最大上限值，不能超过 26 个，因为 iSpirit 3626 交换机的端口个数为 26 个，可以满足应用上的任何要求。

3.私有VLAN和普通VLAN的关系

普通 VLAN 中的一个 VLAN 就是一个广播域，每个 VLAN 可以创建一个子网，VLAN 间通信必须通过三层转发。而私有 VLAN 中一个私有 VLAN 组才是一个广播域，每个私有 VLAN 组可以创建一个子网，在私有 VLAN 组的主 VLAN 之上创建子网，私有 VLAN 组间通信必须通过三层转发，而私有 VLAN 组内通信则是二层转发。

在选择私有 VLAN 组的 VLAN 范围时，要保证该 VLAN 范围中的任何一个 VLAN 都没有被普通 VLAN 占用，如果被占用，则 VLAN 范围选择不成功。在创建普通 VLAN 时，要保证该 VLAN 不在任何私有 VLAN 组中的 VLAN 范围内，如果该 VLAN 在私有 VLAN 组的 VLAN 范围内，则创建不成功。

如果私有 VLAN 组中要设置的混杂端口、共用端口或隔离端口是某个普通 VLAN 的 untagged 成员，则要从该普通 VLAN 中清除该端口，即该端口不再属于该普通 VLAN 的 untagged 成员。

在设置普通 VLAN 的端口成员时，如果一个端口被私有 VLAN 组占用，则该端口不能设置成该 VLAN 的 untagged 成员，但是该端口可以设置成该 VLAN 的 tagged 成员。

在使用命令 show vlan 显示 VLAN 的信息时，只能显示普通 VLAN 的信息，不能显示私有 VLAN 的信息，需要使用 show privatevlan 显示私有 VLAN 的信息。

4.私有VLAN的子网

一个私有 VLAN 组是一个广播域，只能创建一个子网，而且必须在主 VLAN 上创建子网，私有 VLAN 组内的其它 VLAN 不能创建子网。如果一个交换机上有一个私有 VLAN 组，并且创建了子网，只有与混杂端口相连的设备在该子网内能够与该交换机通信，而与隔离端口和共用端口相连的设备在该子网内不能与该交换机通信。在实际应用中，不能把网管工作站建立在私有 VLAN 组的隔离端口或共用端口之下，而必须把网管工作站建立在混杂端口之上。

4.2 私有 VLAN 配置

为了让用户配置私有 VLAN 更加方便，iSpirit 3626 交换机在 CLI 上提供了一个 PRIVATE VLAN 模式，进入 PRIVATE VLAN 模式对一组私有 VLAN 进行配置，私有 VLAN 配置的大部分命令都在 PRIVATE VLAN 模式下运行。

iSpirit 3626 交换机缺省情况下所有的私有 VLAN 组都没有配置任何的 VLAN 和端口。本节描述私有 VLAN 的配置，主要包括以下内容：

- 配置私有 VLAN 组
- 配置私有 VLAN 组内的 VLAN
- 配置私有 VLAN 组内的隔离端口
- 配置私有 VLAN 组内的共用端口
- 配置私有 VLAN 组内的混杂端口
- 使私有 VLAN 组生效和失效
- 显示私有 VLAN 组信息

1.配置私有VLAN组

要对私有 VLAN 进行配置，首先要选择一个私有 VLAN 组并进入 PRIVATE VLAN 模式。

● 下面的命令在全局 CONFIG 模式下选择一个私有 VLAN 组并进入 PRIVATE VLAN 模式，group-id 值为 1 到 12，表示私有 VLAN 组号：

privatevlan <group-id>

● 下面的命令在全局 CONFIG 模式下删除一个私有 VLAN 组，group-id 值为 1 到 12，表示私有 VLAN 组号：

no privatevlan <group-id>

2.配置私有VLAN组内的VLAN

选择了一个私有 VLAN 组并进入 PRIVATE VLAN 模式后，需要选择私有 VLAN 组的 VLAN 范围和主 VLAN。在配置之前，要根据规划计算好需要的 VLAN 个数。

● 下面的命令在 PRIVATE VLAN 模式下选择私有 VLAN 组的 VLAN 范围和主 VLAN，VLAN 范围用最小 VLAN ID 号到最大 VLAN ID 号表示：

vlan <min-vlanid> <max-vlanid> <primary-vlanid>

注意：如果该命令配置不成功，有以下几种可能性：

min-vlanid 值比 max-vlanid 大。

primary-vlanid 不在 min-vlanid 到 max-vlanid 范围内。

max-vlanid 值减 min-vlanid 大于 26。

min-vlanid 值到 max-vlanid 的 VLAN 范围有至少一个 VLAN 被普通 VLAN 占用。

私有 VLAN 组与其它的私有 VLAN 组有 VLAN 范围重叠的现象。

该私有 VLAN 组处于生效（active）状态。

3.配置私有VLAN组内的隔离端口

● 下面的命令在 PRIVATE VLAN 模式下配置一个或多个隔离端口：

isolate {<p>|<p1-p2>} [<p>|<p1-p2>] …

● 下面的命令在 PRIVATE VLAN 模式下清除一个或多个隔离端口，如果被输入的端口不是隔离端口，则对该端口不做任何动作：

no isolate {<p>|<p1-p2>} [<p>|<p1-p2>] …

注意：如果私有 VLAN 组处于生效（active）状态，命令不能设置成功。一个私有 VLAN 组可以不配置隔离端口，但此时需要有一个或多个共用端口组。

4.配置私有VLAN组内的共用端口

● 下面的命令在 PRIVATE VLAN 模式下配置一个共用端口组，一个共用端口组内可以选择一个或多个共用端口，community-id 是共用端口组号：

community <community-id> {<p>|<p1-p2>} [<p>|<p1-p2>] …

● 下面的命令在 PRIVATE VLAN 模式下删除一个共用端口组，此时该共用端口组内的所有共用端口都被清除：

no community <community-id>

注意：

1、如果私有 VLAN 组处于生效（active）状态，命令不能设置成功。

2、一个私有 VLAN 组可以不配置共用端口组，但此时需要有一个或多个隔离端口。

5.配置私有VLAN组内的混杂端口

● 下面的命令在 PRIVATE VLAN 模式下配置一个或多个混杂端口：

promiscuous {<p>|<p1-p2>} [<p>|<p1-p2>] …

● 下面的命令在 PRIVATE VLAN 模式下清除一个或多个混杂端口，如果被输入的端口不是混杂端口，则对该端口不做任何动作：

no promiscuous {<p>|<p1-p2>} [<p>|<p1-p2>] …

注意：

1、如果私有 VLAN 组处于生效（active）状态，命令不能设置成功。

2、一个私有 VLAN 组必须配置一个或多个混杂端口。

6.使私有VLAN组生效和失效

一个私有 VLAN 组配置了 VLAN 和端口后私有 VLAN 组并不立即生效，需要手工输入命令使该私有 VLAN 组生效。

● 下面的命令在 PRIVATE VLAN 模式下使私有 VLAN 组生效：

enable

注意：

如果私有 VLAN 组不能生效，有下面几种可能性：

私有 VLAN 组内的 min-vlanid、max-vlanid 或 primary-vlanid 有为 0 的情况。

私有 VLAN 组内的 VLAN 个数太少，VLAN 个数 < 隔离端口的个数 + 共用端口组的个数 + 1。

私有 VLAN 组内没有混杂端口。

私有 VLAN 组内既没有隔离端口又没有共用端口组。

私有 VLAN 组内混杂端口、共用端口和隔离端口有重叠的现象。

私有 VLAN 组与其它的私有 VLAN 组有混杂端口、共用端口和隔离端口重叠的现象。

如果私有 VLAN 组内的混杂端口、共用端口或隔离端口属于普通 VLAN 的 untagged 成员，则要从该普通 VLAN 中清除这些端口，是这些端口不属于该普通 VLAN 的成员。

● 下面的命令在 PRIVATE VLAN 模式下使私有 VLAN 组失效：

disable

注意：只有在私有 VLAN 组失效时，私有 VLAN 组内的配置才能修改，在私有 VLAN 组生效时，私有 VLAN 组内的配置不能修改，因此当私有 VLAN 组生效时想修改该私有 VLAN 组的配置，首先要使该私有 VLAN 组失效再进行配置，配置完后再使该私有 VLAN 组生效。

7.显示私有VLAN组信息

下面的命令在全局 CONFIG 模式或 PRIVATE VLAN 模式显示私有 VLAN 组的信息，group-id 值为 1 到 12，表示私有 VLAN 组号，如果不输入 group-id 参数，显示所有 12 组私有 VLAN 的配置信息，如果输入 group-id 参数，只显示指定的私有 VLAN 组的配置信息：

show privatevlan [group-id]

第 5 章 配置 STP

本章对 STP 及其配置进行描述，主要包括以下内容：

1、STP 介绍

2、STP 配置

3、STP 配置示例

5.1 STP 介绍

联想天工 iSpirit 3626 交换机支持 IEEE802.1d 标准的 STP 协议。STP 是运行在 Bridges 和 Switches 层上，符合 IEEE802.1d 协议标准兼容的第二层协议。这一协议提供了网络的动态冗余切换机制。因此使用 STP，可以让您在网络设计中部署备份线路，并且保证在主线路正常工作时，备份线路是关闭的。当主线路出现故障时，自动激活备份线路，将数据流切换到备份线路，保证设备正常运行。

由此可见，使用 STP，可以保证当在网络结构上存在冗余路径情况下，阻止网络回路发生。网络回路对网络来说是致命的打击，冗余链路作为网络备份路径又是非常重要的。通过交换机提供的命令可以实现该协议的功能。

5.2 STP 配置

交换机的 STP 功能配置分以下几个步骤：

- 第一步：启用 STP 协议；
- 第二步：对 STP 参数进行设置；

缺省情况下 STP 协议是关闭的，但交换机的所有端口的 STP 计算是打开的。只有在 STP 协议打开并且端口的 STP 计算也打开时，该端口才会真正加入到 STP 计算中，如果有一个条件没有满足，则端口不会加入 STP 计算。

- 在全局配置模式下打开或关闭 STP：

  stp　　　　（打开 STP 协议）

  no stp　　　（关闭 STP 协议）

- 在全局配置模式下使能 STP 端口，使端口用于 STP 计算

  enable stp ports <port|port1-port2> [port|port1-port2] …

- 在全局配置模式下关闭 STP 端口，使端口不用于 STP 运算

  disable stp ports <port|port1-port2> [port|port1-port2] …

- 在全局配置模式下设置桥优先级，其默认值为 32768。

  stp bridge priority <A>

  说明：priority 的范围为 0~65535。

- 在 PORT RANGE 配置模式下设定端口优先级，其默认值为 128。

  stp port priority <A>

  说明：priority 的范围为 0~255。

- 在全局配置模式下设置桥的 BPDU 报文发送周期，默认值为 2 秒。

  stp bridge hello-time <A>

- 在全局配置模式下设置 STP 的转发延迟时间，默认值 15 秒。

  stp bridge forward-delay <A>

- 在全局配置模式下设置桥的 STP 配置信息的最大存活时间，默认值为 20 秒。

  stp bridge max-age <A>

- 在全局配置模式下显示桥的 STP 信息

  show stp bridge

- 在全局配置模式或 PORT RANGE 配置模式下显示某个端口的 STP 信息

  show stp port<port>

第 6 章 配置二层静态组播

本章描述了二层静态组播的概念和配置，包括以下内容：

1、二层静态组播介绍

2、二层静态组播配置

3、二层静态组播配置示例

在城域网/Internet 中，采用单播方式将相同的数据包发送给网络中的多个而不是全部接收者时，由于需要复制分组给每一个接收端点，随着接收者数量的增多，需要发出的包数也会线性增加，这使得主机、交换路由设备及网络带宽资源总体负担加重，效率受到极大影响。随着多点电视会议、视屏点播、群组通信应用等需求的增长，为提高资源利用率，组播方式日益成为多点通信中普遍采用的传输方式。

如图 1 是一个单播应用的例子，实现点到点的通信，如图 2 是一个组播应用的例子，实现点到多点的通信。图 6-1 和图 6-2 都是 A 发送相同内容的数据流给 B 和 C，如果采用单播通信，A 需要发送二个数据流，一个给 B，一个给 C，如果采用组播通信，A 只需要发送一个数据流，B 和 C 都会接收这个数据流。

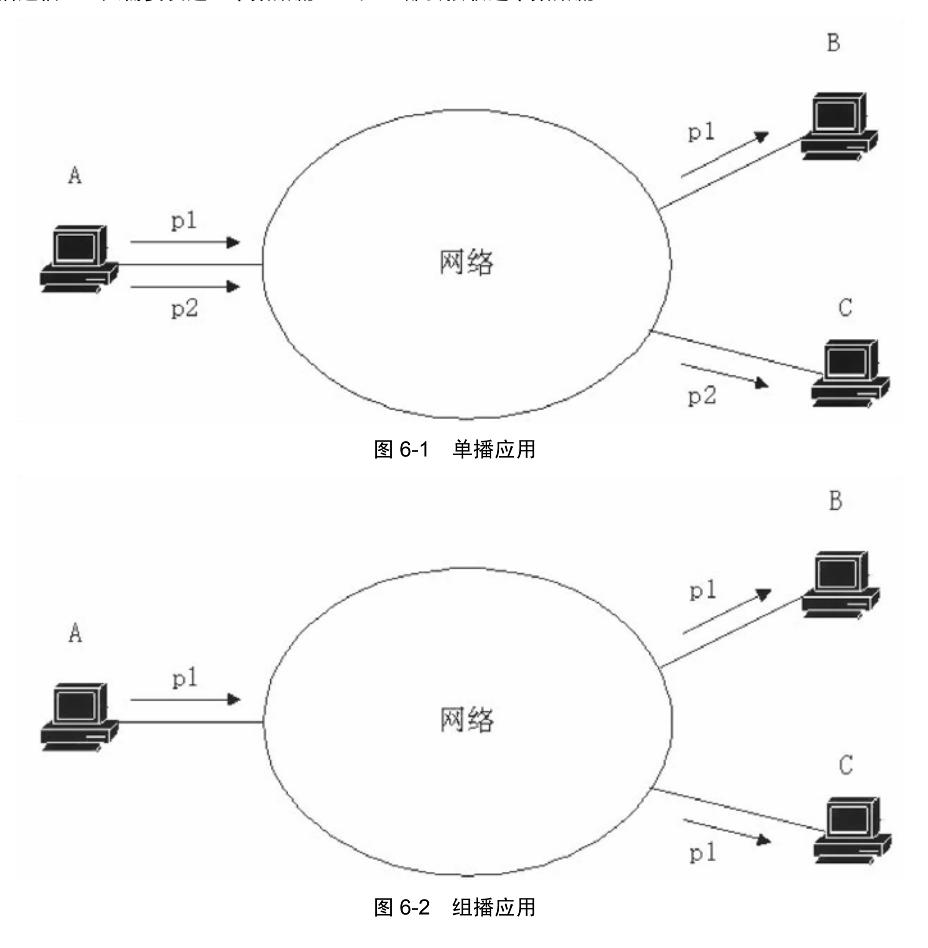


图 6-1　单播应用

图 6-2　组播应用

iSpirit 3626 交换机实现了 IGMP，IGMP SNOOPING 和二层静态组播，这些都是为组播应用服务。IGMP 是组播组管理协议，可以发送 query 报文，维护组播组。IGMP SNOOPING 监听网络上的 IGMP 包，实现 IP 组播 MAC 地址的动态学习。二层静态组播实现手工配置二层组播地址。

6.1 二层静态组播介绍

iSpirit 3626 交换机存在一个二层硬件组播转发表，可以实现二层组播的线速转发。组播 MAC 地址可以通过 IGMP SNOOPING 学习得到，也可以通过手工静态配置得到。

本节包括以下内容：

- 二层硬件组播转发表
- 二层组播 MAC 地址
- 二层组播转发模式
- 二层静态组播和二层动态组播

1.二层硬件组播转发表

二层硬件组播转发表实现二层组播流的线速转发，共有 255 个条目，可以容纳 255 个组播 MAC 地址。二层硬件组播转发表的每个条目有三个重要的字段，分别是：组播 MAC 地址、VLAN ID 和输出端口列表，其中索引是组播 MAC 地址和 VLAN ID 号。

在二层硬件组播转发表中多个 VLAN（也就是多个子网）可以存在相同的组播 MAC 地址，需要有多个条目来容纳。当二层组播流从交换机的一个端口输入时，首先得到二层组播流的组播 MAC 地址和所属的 VLAN ID，查找二层硬件组播转发表，如果匹配了一个条目，把输出端口列表取出来，去除输入端口，二层组播流从这些端口发出去。输出端口列表中可以没有输出端口或只有一个输出端口或有多个输出端口。

2.二层组播MAC地址

MAC 地址分为组播 MAC 地址和单播 MAC 地址，组播 MAC 地址的最高字节的最低位为 1，单播 MAC 地址的最高字节的最低位为 0，如图 6-3 所示。例如地址 01:00:00:00:00:01 是组播 MAC 地址，地址 00:00:00:00:00:01 是单播 MAC 地址。

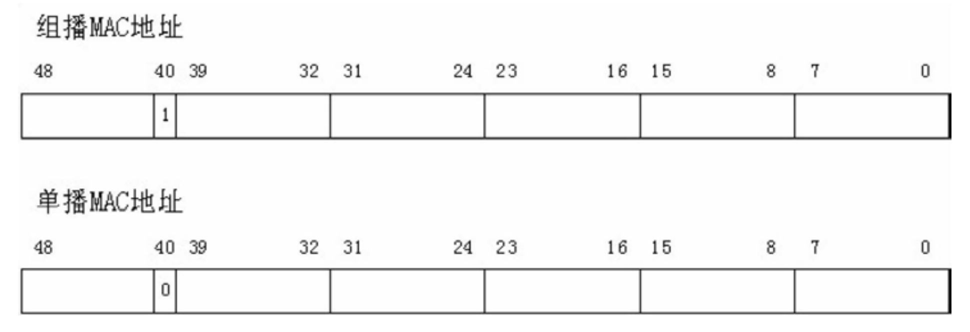


图 6-3　组播和单播 MAC 地址

组播 MAC 地址又分为 IP 组播 MAC 地址和非 IP 组播 MAC 地址。IP 组播 MAC 地址是三层 IP 组播地址映射成的组播 MAC 地址，其中前三个字节必须是 01:00:5e，第 23 位必须为 0，其它 23 位地址是三层 IP 组播地址的低 23 位

映射而成。非 IP 组播 MAC 地址是除了 IP 组播 MAC 地址以外的所有组播 MAC 地址。例如 01:00:5e:00:00:01 是 IP 组播 MAC 地址，而 01:00:ff:00:00:01 是非 IP 组播 MAC 地址。如图 4 所示为 IP 组播 MAC 地址。

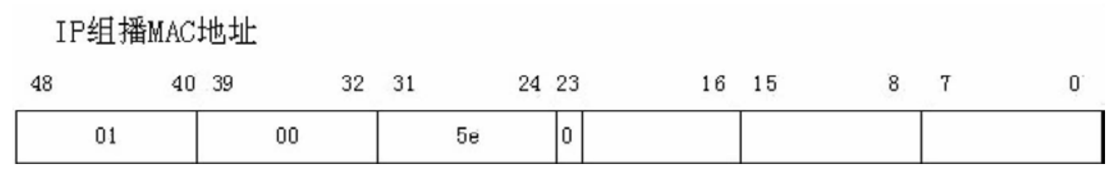


图 4 IP 组播 MAC 地址

3.二层组播转发模式

二层硬件组播转发表存在两种组播转发模式，分别是：未注册转发模式和注册转发模式。

对于未注册转发模式，当二层组播数据流从二层硬件组播转发表中找到匹配的条目，则根据该条目的输出端口列表进行转发，如果没有找到匹配的条目，则向该 VLAN 的所有其它端口转发，此时相当于广播。

对于注册转发模式，当二层组播数据流从二层硬件组播转发表中找到匹配的条目，则根据该条目的输出端口列表进行转发，如果没有找到匹配的条目，则丢弃该二层组播数据流。

iSpirit 3626 交换机上如果 IGMP SNOOPING 是关闭的，二层组播处于未注册转发模式，如果 IGMP SNOOPING 是打开的，二层组播处于注册转发模式。

4.二层静态组播和二层动态组播

二层硬件组播转发表中的组播 MAC 地址条目可以通过 IGMP SNOOPING 动态学习得到，也可以通过手工配置。通过 IGMP SNOOPING 动态学习到的是 IP 组播 MAC 地址，而通过手工配置的可以是 IP 组播 MAC 地址，也可以是非 IP 组播 MAC 地址。

当交换机关闭 IGMP SNOOPING 时，二层硬件组播转发表处于未注册转发模式，组播 MAC 地址不能动态学习到，二层硬件组播转发表中没有条目，所有的二层组播数据流当作广播处理。此时可以通过手工往二层硬件组播转发表中加静态组播条目，可以控制二层组播数据流只往指定的端口输出转发，减小网络的组播流量。

当网络具备组播环境时，为了有效控制网络的组播流量，交换机可以打开 IGMP SNOOPING，此时二层硬件组播转发表处于注册转发模式，交换机可以通过监听网络上的 IGMP 协议包学习到组播 MAC 地址，与二层硬件组播转发表中的条目匹配的二层组播流才能够转发。为了让学习不到的组播 MAC 地址的二层组播流得到转发，可以通过手工往二层硬件组播转发表中加静态组播条目。

当静态配置和动态学习到的 IP 组播 MAC 地址是二层硬件组播转发表中的同一个条目时，输出端口列表包括静态配置的端口和动态学习的端口。当删除静态配置的 IP 组播 MAC 地址时，只去除静态配置的端口，动态学习到的端口继续保留，当动态学习到的 IP 组播 MAC 地址不再存在时，只去除动态学习到的端口，静态配置的端口继续保留。

6.2 二层静态组播配置

iSpirit 3626 交换机缺省情况下没有二层静态组播配置。本节描述二层静态组播的配置，主要包括以下内容：

- 配置二层组播地址
- 显示二层组播地址信息

1.配置二层组播地址

二层组播地址的配置非常简单，包括创建二层组播地址条目和增加二层组播地址条目的输出端口，删除二层组播地址条目和删除二层组播地址条目的输出端口。

● 下面的命令在全局 CONFIG 模式下创建二层组播地址条目和增加二层组播地址条目的输出端口，需要输入 VLAN ID、组播 MAC 地址和输出端口列表。如果该二层组播条目不存在，则创建一个二层组播条目，并把指定的端口列表当作该条目的输出端口列表。如果该二层组播条目存在，则把指定的端口列表增加到该条目的输出端口列表中。

multicast <vlanid> <mac-address> {<port>|<port1-port2>} [<port>|
<port1-port2>] …

● 下面的命令在全局 CONFIG 模式下删除二层组播地址条目和删除二层组播地址条目的输出端口，需要输入 VLAN ID 和组播 MAC 地址，端口可以输入也可以不输入。如果不输入端口，则删除此二层组播地址条目，该条目中所有的输出端口列表都被清除。如果输入端口，则从此二层组播地址条目的输出端口列表中去除指定的端口。

no multicast <vlanid> <mac-address> [<port>|<port1-port2>] …

2.显示二层组播地址信息

二层组播地址包括静态配置的二层组播地址和动态学习到的二层组播地址，iSpirit 3626 交换机提供了两个二层组播地址的显示命令，一个显示静态配置的二层组播地址信息，另一个显示所有的二层组播地址信息，包括静态配置的和动态学习到的。

● 下面的命令在全局 CONFIG 模式下显示静态配置的二层组播地址信息：

show multicast static

● 下面的命令在全局 CONFIG 模式下显示所有的二层组播地址信息：

show multicast

第 7 章 配置 IGMP SNOOPING

本章对 IGMP SNOOPING 的概念和配置进行描述，主要包括以下内容：

1、IGMP SNOOPING 介绍

2、IGMP SNOOPING 配置

3、IGMP SNOOPING 配置示例

在城域网/Internet 中，采用单播方式将相同的数据包发送给网络中的多个而不是全部接收者时，由于需要复制分组给每一个接收端点，随着接收者数量的增多，需要发出的包数也会线性增加，这使得主机、交换路由设备及网络带宽资源总体负担加重，效率受到极大影响。随着多点电视会议、视屏点播、群组通信应用等需求的增长，为提高资源利用率，组播方式日益成为多点通信中普遍采用的传输方式。

iSpirit 3626 交换机实现了 IGMP，IGMP SNOOPING 和二层静态组播，这些都是为组播应用服务。IGMP 是组播组管理协议，实现直连子网内的三层 IP 组播地址的动态学习。IGMP SNOOPING 监听网络上的 IGMP 包，实现 IP 组播 MAC 地址的动态学习。二层静态组播实现手工配置二层组播地址。

7.1 IGMP SNOOPING 介绍

传统的网络在一个子网内组播数据包当作广播处理，这样容易使网络流量大，造成网络拥塞。当交换机上实现了 IGMP SNOOPING 后，IGMP SNOOPING 可以动态学习 IP 组播 MAC 地址，维护 IP 组播 MAC 地址的输出端口列表，使组播数据流只往输出端口发送，这样可以减少网络的流量。

二层静态组播是通过手工配置二层组播地址，而 IGMP SNOOPING 是通过动态学习二层组播地址，两者之间有密切的关系。二层静态组播请参见“配置二层静态组播”章节。本节主要包括以下内容：

- IGMP SNOOPING 处理过程
- 二层动态组播和二层静态组播
- 加入一个组
- 离开一个组

1. IGMP SNOOPING处理过程

IGMP SNOOPING 是一个二层的网络协议，监听经过交换机的 IGMP 协议包，根据这些 IGMP 协议包的收包端口，vlanid，组播地址来维护一个组播组，然后转发这些 IGMP 协议包。只有加入了组播组的端口才可以接收组播数据流；这样就减少了网络的流量，节省了网络带宽。

组播组包括了组播组地址，成员端口，VlanId，Age，Type 字段。

IGMP SNOOPING 组播组的形成是一个学习的过程。当交换机的某一个端口收到 IGMP REPORT 包时，IGMP SNOOPING 会产生一个新的组播组，接收 IGMP REPORT 包的端口就被加入这个组播组。在交换机收到一个 IGMP QUERY 包时，如果这个组播组已经存在交换机中，那么这个收到 IGMP QUERY 的端口也加入到这个组播组中，否则只是转发 IGMP QUERY 包。IGMP SNOOPING 还支持 IGMP V2 的 Leave 机制；如果 IGMP SNOOPING 配置了 immediate leave 为 ENABLE，在收到 IGMP V2 的 leave 包时收包端口可以立刻离开组播组。

IGMP SNOOPING 有两种更新机制。一种是上面介绍的 leave 机制。大多数情况下 IGMP SNOOPING 是通过 age

time 来删除过期的组播组的。当组播组加入 IGMP SNOOPING 时记录了加入的时间，当组播组在交换机中存留的时间超过了一个配置的 age time 时，交换机会删除这个组播组。

2．二层动态组播和二层静态组播

二层硬件组播转发表中的组播 MAC 地址条目可以通过 IGMP SNOOPING 动态学习得到，也可以通过手工配置。通过 IGMP SNOOPING 动态学习到的是 IP 组播 MAC 地址，而通过手工配置的可以是 IP 组播 MAC 地址，也可以是非 IP 组播 MAC 地址。

当交换机关闭 IGMP SNOOPING 时，二层硬件组播转发表处于未注册转发模式，组播 MAC 地址不能动态学习到，二层硬件组播转发表中没有条目，所有的二层组播数据流当作广播处理。此时可以通过手工往二层硬件组播转发表中加静态组播条目，可以控制二层组播数据流只往指定的端口输出转发，减小网络的组播流量。

当网络具备组播环境时，为了有效控制网络的组播流量，交换机可以打开 IGMP SNOOPING，此时二层硬件组播转发表处于注册转发模式，交换机可以通过监听网络上的 IGMP 协议包学习到组播 MAC 地址，与二层硬件组播转发表中的条目匹配的二层组播流才能够转发。为了让学习不到的组播 MAC 地址的二层组播流得到转发，可以通过手工往二层硬件组播转发表中加静态组播条目。

当静态配置和动态学习到的 IP 组播 MAC 地址是二层硬件组播转发表中的同一个条目时，输出端口列表包括静态配置的端口和动态学习的端口。当删除静态配置的 IP 组播 MAC 地址时，只去除静态配置的端口，动态学习到的端口继续保留，当动态学习到的 IP 组播 MAC 地址不再存在时，只去除动态学习到的端口，静态配置的端口继续保留。

3．加入一个组

当一个主机想加入一个组播组时，主机会发一个 IGMP REPORT 包，在此包中指定主机要加入的组播组。当交换机收到一个 IGMP QUERY 包时，交换机会把该包转发给同一个 VLAN 的所有其它端口，当端口下的想加入组播组的主机收到 IGMP QUERY 包后会回送一个 IGMP REPORT 包。当交换机收到一个 IGMP REPORT 包后，会建立一个二层组播条目，收到 IGMP QUERY 包的端口和 IGMP REPORT 包的端口会加入到该二层组播条目，成为它的输出端口。

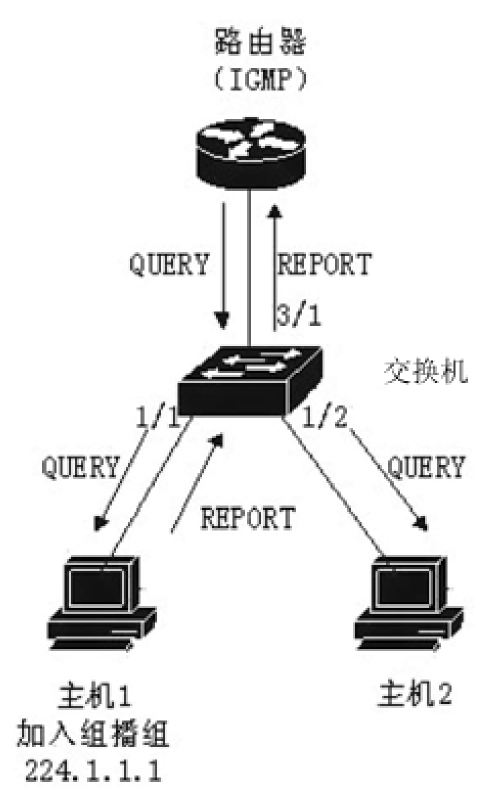


图 7-1 主机 1 加入组播组

如图 7-1 所有的设备在一个子网内，假设该子网的 VLAN 是 2。路由器运行 IGMPv2 协议，定时发送 IGMP QUERY 包。主机 1 想加入组播组 224.1.1.1。交换机从 3/1 端口收到 IGMP QUERY 包后会记录此端口并把该包转发给端口 1/1 和 1/2。主机 1 收到 IGMP QUERY 包后回送一个 IGMP REPORT 包，主机 2 因为不想加入组播组，不发 IGMP REPORT 包。交换机从端口 1/1 收到 IGMP REPORT 包后会把该包从查询端口 3/1 转发出去并且创建一个二层组播条目（假定该条目不存在），该二层组播条目包括以下几项：

表 7-1：

二层组播地址	VLAN ID	输出端口列表
01:00:5e:01:01:01	2	1/1，3/1

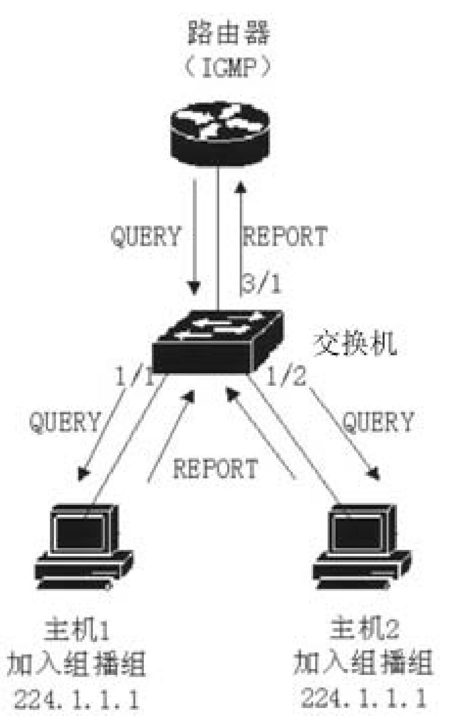


图 7-2　主机 1 和主机 2 加入组播组

如图 7-2 的条件与图 7-1 一样，主机 1 已经加入了组播组 224.1.1.1，现在主机 2 想加入组播组 224.1.1.1。当主机 2 收到 IGMP QUERY 包后回送一个 IGMP REPORT 包，交换机从端口 1/2 收到 IGMP REPORT 后会把该包从查询端口 3/1 转发出去并且会包端口 1/2 加入到二层组播条目中，该二层组播条目变为：

表 7-2：

二层组播地址	VLAN ID	输出端口列表
01:00:5e:01:01:01	2	1/1，1/2，3/1

4．离开一个组

为了能够组成一个稳定的组播环境，运行 IGMP 的设备（如路由器）会每隔一定的时间发送一个 IGMP QUERY 包给所有的主机。已经加入组播组或想加入组播组的主机收到该 IGMP QUERY 后会回送一个 IGMP REPORT。

如果主机想离开一个组播组，可以有两种方式：主动离开和被动离开。主动离开就是主机发送一个 IGMP LEAVE 包给路由器，被动离开就是当主机收到路由器发来的 IGMP QUERY 后不回送 IGMP REPORT。

与主机离开组播组的方式对应，在交换机上端口脱离二层组播条目的方式也有两种：超时离开和收到 IGMP LEAVE 包离开。

当交换机超过一定的时间没有从一个端口收到一个组播组的 IGMP REPORT 包时，该端口要从对应的二层组播条目中清除，如果该二层组播条目没有了端口，则删除此二层组播条目。

当交换机的 immediate leave 配置为 ENABLE 时，如果某个端口收到一个组播组的 IGMP LEAVE 包时，该端口从对应的二层组播条目中清除，如果该二层组播条目没有了端口，则删除此二层组播条目。immediate leave 一般应用

在一个端口下接一个主机的情况。

7.2 IGMP SNOOPING 配置

本节介绍 IGMP SNOOPING 的配置，主要包括以下内容：

- IGMP SNOOPING 缺省配置
- 打开和关闭 IGMP SNOOPING
- 打开和关闭 immediate leave
- 配置组播组 age 时间
- 显示组播组信息

1. IGMP SNOOPING缺省配置

IGMP SNOOPING 缺省是关闭的，二层硬件组播转发表处于未注册转发模式。

immediate leave 缺省是关闭的。

组播组 age 时间缺省为 300 秒。

2.打开和关闭IGMP SNOOPING

下面的命令在全局 CONFIG 模式下打开 IGMP SNOOPING，会往所有端口的 FFP 中加一个条目：

igmp snooping

下面的命令在全局 CONFIG 模式下关闭 IGMP SNOOPING：

no igmp snooping

3.打开和关闭immediate leave

- 下面的命令在全局 CONFIG 模式下打开 immediate leave：

  igmp snooping immediate-leave

- 下面的命令在全局 CONFIG 模式下关闭 immediate leave：

  no igmp snooping immediate-leave

4.配置组播组age时间

下面的命令在全局 CONFIG 模式下设置组播组的 age 时间，单位为秒

igmp snooping age <age-interval>

5.显示组播组信息

- 下面的命令在全局 CONFIG 模式下显示 IGMP SNOOPING 的所有信息：

  show igmp snooping

- 下面的命令在全局 CONFIG 模式下显示所有的二层组播组的信息，包括 IGMP SNOOPING 学习到的和静态配置的二层组播条目：

  show multicast

第 8 章 配置 AAA

本章描述如何配置 iSpirit 3626 交换机的 802.1x 和 RADIUS 以防止非法用户接入网络。关于 802.1x 客户端和 HyperBoss 的使用请参见各自的操作手册。本章主要包括以下内容：

1、802.1x 介绍

2、RADIUS 介绍

3、配置 802.1x

4、配置 RADIUS

AAA 是认证，授权和计费（Authentication, Authorization, and Accounting）的简称。它提供了一个用来对认证，授权和计费这三种安全功能进行配置的一致的框架。AAA 的配置实际上是对网络安全的一种管理，这里的网络安全主要指访问控制。包括哪些用户可以访问网络？具有访问权的用户可以得到哪些服务？如何对正在使用网络资源的用户进行记账？

- 认证(Authentication): 验证用户是否可以获得访问权。
- 授权(Authorization) : 授权用户可以使用哪些服务。
- 计费(Accounting) : 记录用户使用网络资源的情况。

联想网络公司推出了一整套 AAA 的解决方案，产品有 802.1x 客户端、各种支持认证的交换机和认证计费系统 HyperBoss。802.1x 客户端安装在用户上网的 PC 机上，当用户需要访问网络时，需要使用 802.1x 客户端进行认证，只有通过认证的用户才能使用网络。iSpirit 3626 是一款支持认证的交换机，它接收客户端的认证请求，把用户名和口令传送给认证计费系统 HyperBoss，交换机本身不做实际的认证工作。HyperBoss 接收交换机发来的认证请求进行实际的认证，并对认证成功的用户进行计费处理。

在 802.1x 客户端和交换机之间使用 802.1x 协议进行通信，在交换机和 HyperBoss 之间使用 RADIUS 协议进行通信。

8.1 802.1x 介绍

802.1x 协议是一个基于端口的访问控制和认证协议，这里指的端口是逻辑端口，可以是物理端口、MAC 地址或 Vlan ID 等，联想网络的交换机实现的都是基于 MAC 地址的 802.1x 协议。

802.1x 是一个二层协议，认证的交换机和用户的 PC 机必须处于同一个子网中，协议包不能跨越网段。802.1x 认证采用的是客户服务器的模型，必须有一个服务器对所有的用户进行认证。在用户通过认证之前，只有认证流能够通过交换机的端口，在认证成功后，数据流才能通过交换机的端口，也就是说用户必须在认证通过后才能访问网络。

本节主要包括以下内容：

- 802.1x 设备组成
- 协议包简介
- 协议流交互
- 802.1x 端口状态

1. 802.1x设备组成

802.1x 设备由三部分组成：客户端（Supplicant System）、认证系统（Authenticator System）和认证服务器（Authentication Server System）。如图 8-1 所示。

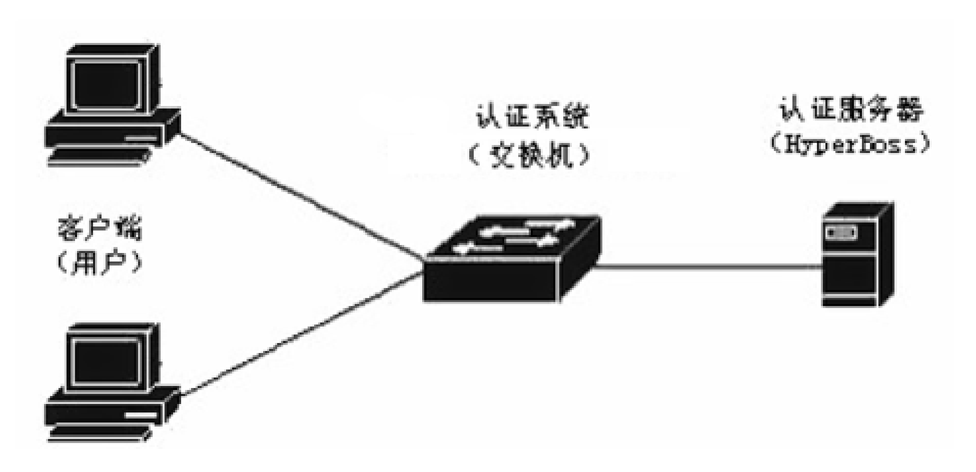


图 8-1　802.1x 设备

客户端指的是请求访问网络的设备，一般是用户终端系统，如用户的 PC 机，在用户终端系统上必须要安装一个 802.1x 客户端软件，该软件实现 802.1x 协议中的客户端部分。客户端发起 802.1x 认证请求，请求认证服务器对其用户名和口令进行验证，如果认证成功，用户可以访问网络。

认证系统指的是认证的设备，如 iSpirit 3626 交换机。认证系统通过用户的逻辑端口（指的是 MAC 地址）的状态控制用户是否可以访问网络，如果用户的逻辑端口状态是非授权的，则用户不可以访问网络，如果用户的逻辑端口状态是授权的，则用户可以访问网络。

认证系统是客户端和认证服务器之间的一个中继。认证系统请求用户的身份信息，并把用户的身份信息转发给认证服务器，并把认证服务器发来的认证结果转发给客户端。认证系统在靠近用户端要实现 802.1x 协议的服务端部分，在靠近认证服务器端要实现 RADIUS 协议的客户端部分，认证系统的 RADIUS 协议客户端把 802.1x 客户端送来 EAP 信息封装在 RADIUS 中发送给认证服务器，并从认证服务器发来的 RAIDUS 协议包中把 EAP 信息解封装出来并通过 802.1x 服务端部分传送给 802.1x 客户端。

认证服务器指的是实际对用户进行认证的设备。认证服务器接收认证系统发来的用户的身份信息并进行验证，如果认证成功，认证服务器对认证系统进行授权，允许用户访问网络，如果认证失败，认证服务器告诉认证系统用户认证失败，用户不能访问网络。认证服务器和认证系统之间通过 EAP 扩展的 RADIUS 协议进行通信。联想网络提供了认证计费系统 HyperBoss 对用户进行认证和计费。

2.协议包简介

802.1x 协议在网络上传输的认证数据流是 EAPOL（EAP Over LAN）帧格式，所有的用户身份信息（包括用户名和口令）封装在 EAP（扩展认证协议）中，EAP 再封装在 EAPOL 帧中。用户名以明文的形式在 EAP 中存在，而口令则以 MD5 加密的形式在 EAP 中存在。

EAPOL 帧格式如图 8-2。PAE Ethernet Type 是 EAPOL 的以太网协议类型号，值为 0x888E。Protocol Version 是 EAPOL 版本号，值为 1。Packet Type 指的是 EAPOL 帧类型。Packet Body Length 是 EAPOL 帧内容的长度。Packet Body 指的是 EAPOL 帧的内容。

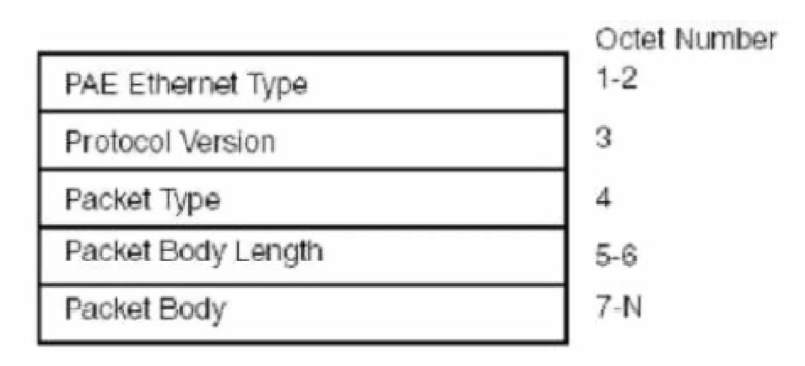


图 8-2　EAPOL 帧格式

联想交换机使用了三种 EAPOL 协议帧，分别是：

EAPOL-Start：Packet Type 的值为 1，认证发起帧，当用户需要进行认证时首先发起此帧，由客户端发给交换机。

EAPOL-Logoff：Packet Type 的值为 2，退出请求帧，当用户不需要使用网络时发此帧通知交换机。

EAP-Packet：Packet Type 的值为 0，认证信息帧，用于承载认证信息。

EAP 包格式如图 3。Code 指的是 EAP 包的类型，包括 Request、Response、Success 和 Failure。Identifier 指的是标识符，用于匹配 Response 和 Request。Length 指的是 EAP 包长度，包括包头。Data 指的是 EAP 包数据。

EAP 包包括以下四种类型：

EAP-Request：Code 值为 1，EAP 请求包，从交换机发给客户端请求用户名和（或）口令。

EAP-Response：Code 值为 2，EAP 应答包，从客户端发给交换机，把用户名和（或）口令送给交换机。

EAP-Success：Code 值为 3，EAP 成功包，从交换机发给客户端，告诉客户端用户认证成功。

EAP-Failure：Code 值为 4，EAP 失败包，从交换机发给客户端，告诉客户端用户认证失败。

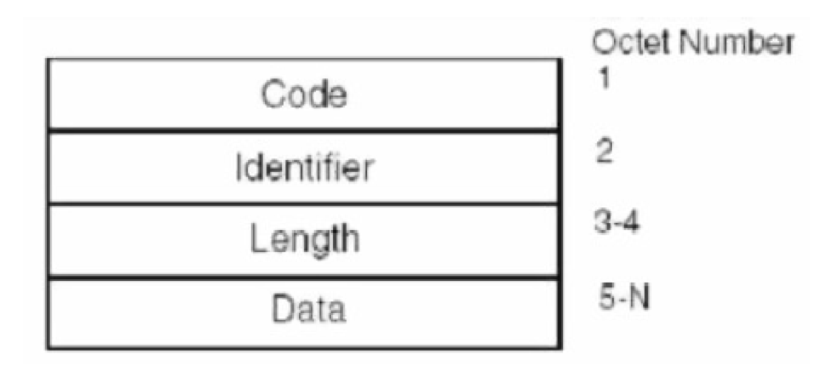


图 8-3　EAP 包格式

3.协议流交互

当交换机使能 802.1x 并且端口的状态是 Auto 时，该端口下的所有接入用户都必须通过认证后才能访问网络。协议交互如图 8-4。

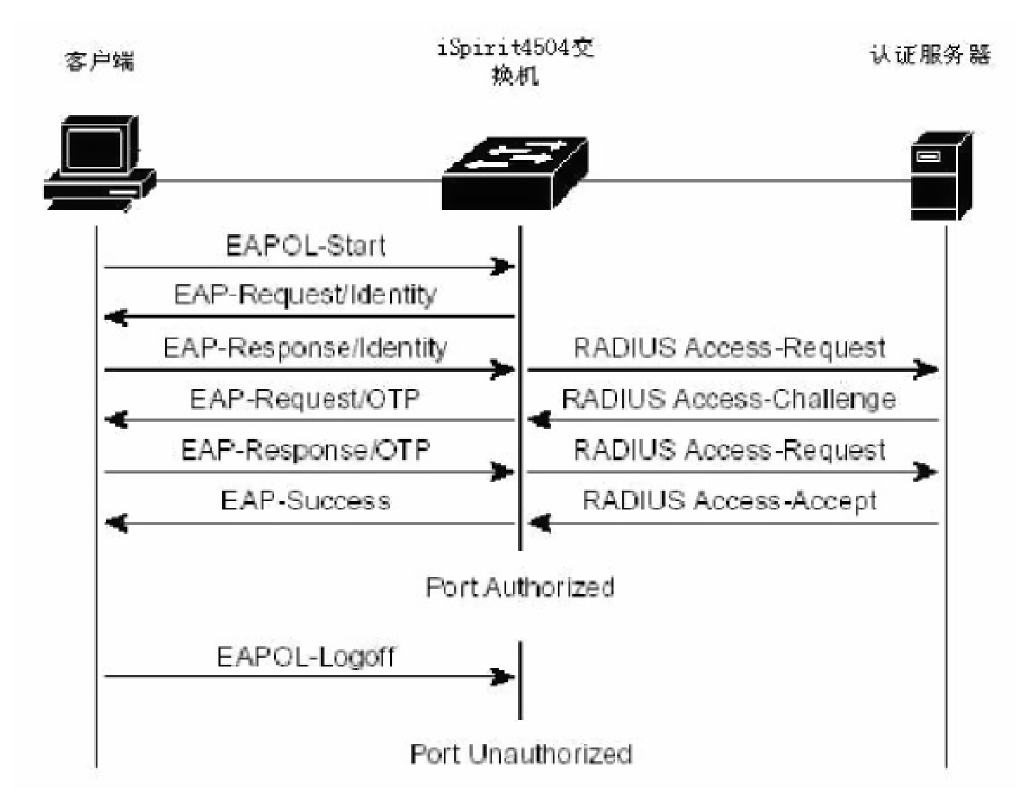


图 8-4　客户端发起认证的协议交互

当用户需要访问网络时，客户端首先发送 EAPOL-Start 给交换机请求认证，交换机收到认证请求后发送 EAP-Request 请求用户的用户名，客户端回送 EAP-Response，交换机把 EAP 信息提取出来封装在 RADIUS 包中发给认证服务器，认证服务器请求用户的口令，交换机发送 EAP-Request 给客户端请求用户的口令，客户端回送 EAP-Response，交换机把 EAP 信息封装在 RADIUS 包中发送给认证服务器，认证服务器根据用户名和口令对用户进行认证。如果认证成功，认证服务器通知交换机，交换机发 EAP-Success 给客户端并把用户的逻辑端口处于授权状态。当客户端收到 EAP-Success 后表示认证成功，用户可以访问网络。

当用户不再需要使用网络，客户端发送 EAPOL-Logoff 给交换机，交换机把用户的逻辑端口状态迁为非授权状态，此时用户不能访问网络。

为了防止客户端异常下线，iSpirit 3626 交换机提供了重新认证的机制，可以在交换机上设定重新认证的间隔时间，当认证时间到达，交换机发起重新认证，如果认证成功，用户可以继续使用网络，如果认证失败，用户将不能使用网络。协议交互如图 8-5。

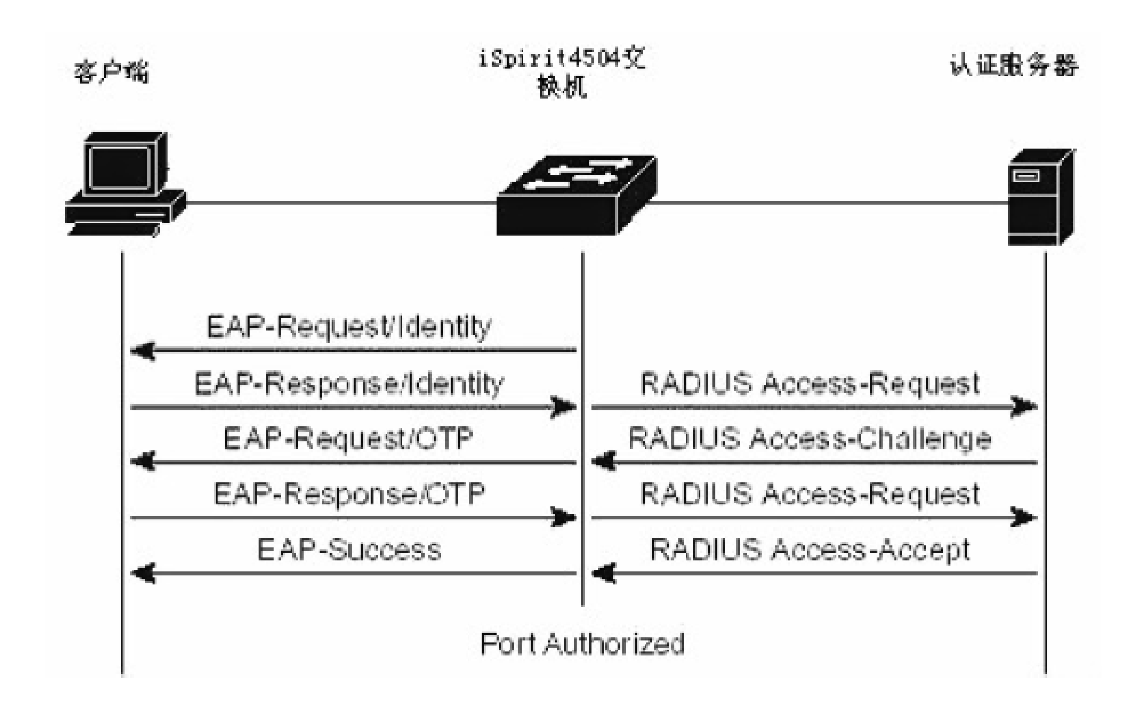


图 8-5 重新认证的协议交互

4. 802.1x端口状态

这里指的端口状态是交换机的物理端口状态。交换机的物理端口存在四种状态：N/A 状态、Auto 状态、Force-authorized 状态和 Force-unauthorized 状态。当交换机没有打开 802.1x 时，所有的端口处于 N/A 状态。当交换机端口要设置成 Auto 状态、Force-authorized 状态或 Force-unauthorized 状态时，必须先使能交换机的 802.1x。

当交换机的端口处于 N/A 状态时，端口下的所有用户不需要认证就可以访问网络。当交换机从该端口收到 802.1x 协议包时，丢弃这些协议包。

当交换机的端口处于 Force-authorized 状态时，端口下的所有用户不需要认证就可以访问网络。当交换机从该端口收到 EAPOL-Start 包，交换机回送 EAP-Success 包，当交换机从该端口收到其它的 802.1x 协议包，丢弃这些协议包。

当交换机的端口处于 Force-unauthorized 状态时，端口下的所有用户始终不能访问网络，认证请求永远通不过。当交换机从该端口收到 802.1x 协议包时，丢弃这些协议包。

当交换机的端口处于 Auto 状态时，端口下的所有用户必须通过认证后才能访问网络。802.1x 协议交互如图 4。如果用户需要做认证，端口一般要设置成 Auto 状态。当交换机端口设置成 Auto 状态时，交换机要占用该端口 FFP 中的 RULE 表的一个条目。

8.2 RADIUS 介绍

当用户进行认证时，交换机和认证服务器之间采用支持 EAP 扩展的 RADIUS 协议进行交互。RADIUS 协议采用客户/服务器模型，交换机需要实现 RADIUS 客户端，而认证服务器需要实现 RADIUS 服务端。

为了保证交换机和认证服务器之间交互的安全性，防止非法的交换机或非法的认证服务器之间的交互，交换机和

认证服务器之间要相互鉴权。交换机和认证服务器需要一个相同的密钥，当交换机或认证服务器发送 RADIUS 协议包时，所有的协议包要根据密钥采用 HMAC 算法生成消息摘要，当交换机和认证服务器收到 RADIUS 协议包时，所有的协议包的消息摘要要使用密钥进行验证，如果验证通过，认为是合法的 RADIUS 协议包，否则是非法的 RADIUS 协议包，丢弃。

本节主要包括以下内容：

- 协议包简介
- 协议流交互
- 用户验证方法

1.协议包简介

RADIUS 是建立在 UDP 之上的协议，RADIUS 可以封装认证信息和计费信息。早期的 RADIUS 认证端口是 1645，目前使用端口 1812，早期的 RADIUS 计费端口是 1646，目前使用端口 1813。

因为 RADIUS 承载在 UDP 上， 所以 RADIUS 要有超时重发机制。同时为了提高认证系统与 RADIUS 服务器通信的可靠性，一般采用两个 RADIUS 服务器方案，即采用备用服务器机制。

RADIUS 报文格式如图 6。Code 指 RADIUS 协议报文类型。Identifier 指标识符，用于匹配请求和应答。Length 指整个报文（包括报文头）的长度。Authenticator 是一个 16 字节的串，对于请求包是一个随机数，对于应答包是 MD5 生成的消息摘要。Attribute 指 RADIUS 协议包中的属性。

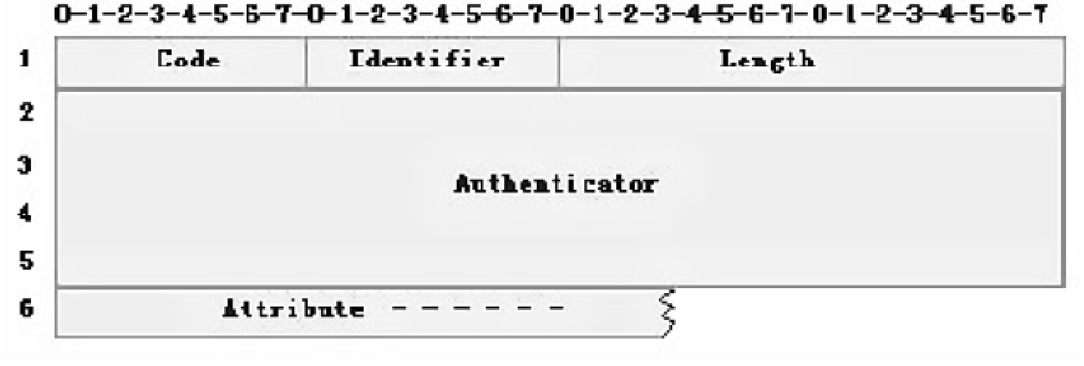


图 8-6　RADIUS 报文格式

联想网络使用了以下几种 RADIUS 协议包：

- Access-Request：Code 值为 1，从认证系统发给认证服务器的认证请求包，用户名和口令封装在此包上。
- Access-Accept：Code 值为 2，从认证服务器发给认证系统的应答包，表示用户认证成功。
- Access-Reject：Code 值为 3，从认证服务器发给认证系统的应答包，表示用户认证失败。
- Access-Challenge：Code 值 11，从认证服务器发给认证系统的应答包，表示认证服务器需要用户的进一步的信息，如口令等。
- Accounting-Request：Code 值为 4，从认证系统发给认证服务器的计费请求包，包括开始计费和结束计费包，计费信息封装在此包上。

- Accounting-Response：Code 值为 5，从认证服务器发给认证系统的计费应答包，表示计费信息已收到。

2.协议流交互

当用户发起认证后认证系统和认证服务器之间通过 RADIUS 协议进行交互。认证系统不发 RADIUS 计费包的协议流交互如图 8-4。一般情况下，在用户认证成功后或用户下线时，认证系统需要给认证服务器发 RADIUS 计费包，协议流交互如图 8-7 所示。

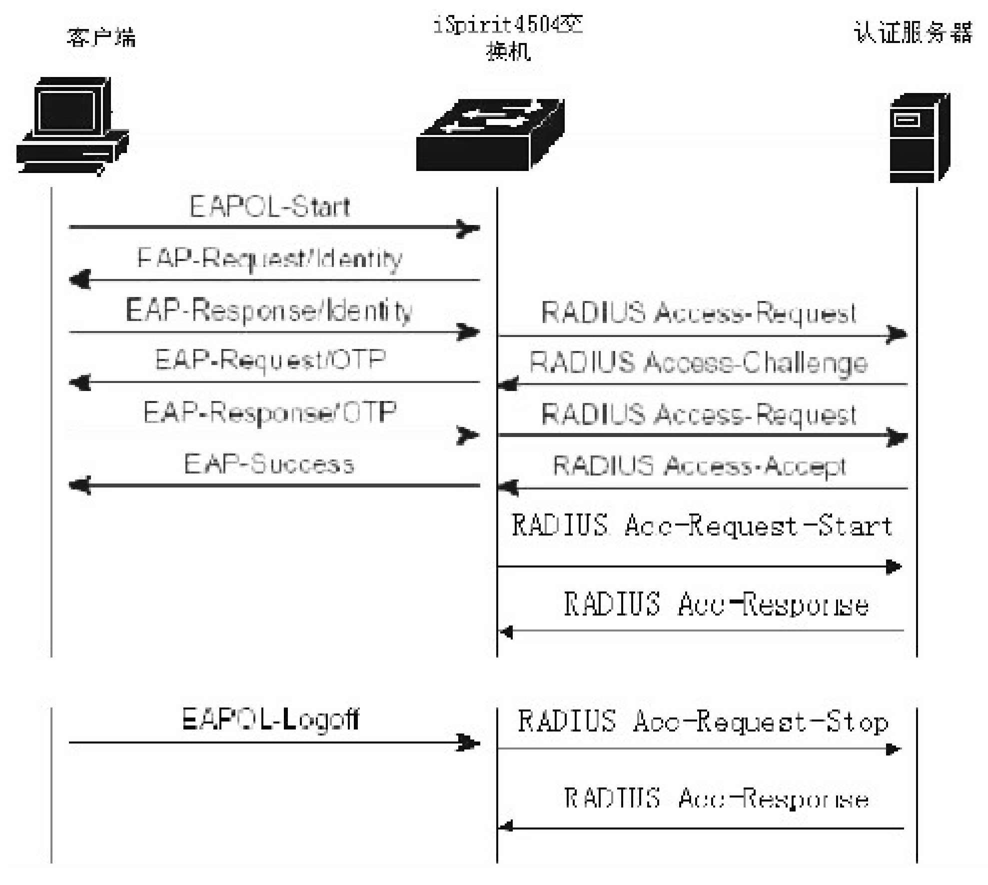


图 8-7 协议流交互

用户进行认证时，交换机把用户名封装在 Access-Request 报文中发给认证服务器，服务器应答 Access-Challenge 请求用户的口令，交换机请求客户端用户的口令，客户端把口令封装在 EAP 中，交换机获取到此 EAP 后封装在 Access-Request 发给认证服务器，认证服务器对用户进行认证，如果认证成功，回送 Access-Accept 给交换机，交换机收到此报文后通知客户端认证成功，同时发送 Accounting-Request 通知认证服务器开始计费，认证服务器回送 Accounting-Response。

当用户不想使用网络时，通知交换机用户下线，交换机发 Accounting-Request 通知认证服务器结束计费，计费信息封装在此包中，认证服务器回送 Accounting-Response。

3.用户验证方法

RADIUS 有三种用户验证方法，如下：

PAP（Password Authentication Protocol）。用户以明文的形式把用户名和他的密码传递给交换机。 交换机通过 RADIUS 协议包把用户名和密码传递给 RADIUS 服务器，RADIUS 服务器查找数据库，如果存在相同的用户名和密码表明验证通过,否则表明验证未通过。

CHAP（Challenge Handshake Authentication Protocol）。当用户请求上网时，交换机产生一个 16 字节的随机码给用户。用户对随机码，密码以及其它各域加密生成一个 response，把用户名和 response 传给交换机。交换机把用户名，response 以及原来的 16 字节随机码传给 RADIUS 服务器。RADIU 根据用户名在交换机端查找数据库，得到和用户端进行加密所用的一样的密码，然后根据传来的 16 字节的随机码进行加密，将其结果与传来的 response 作比较，如果相同表明验证通过，如果不相同表明验证失败。

EAP（Extensible Authentication Protocol）。用此种验证方法，交换机并不真正参与验证，只起到用户和 RADIUS 服务器之间的转发作用。当用户请求上网时，交换机请求用户的用户名，并把用户名转送给 RADIUS 服务器，RADIUS 服务器产生一个 16 字节的随机码给用户并存储该随机码，用户对随机码，密码以及其它各域加密生成一个 response，把用户名和 response 传给交换机，交换机转发给 RADIUS 服务器。 RADIU 根据用户名在交换机端查找数据库，得到和用户端进行加密所用的一样的密码，然后根据存储的 16 字节的随机码进行加密，将其结果与传来的 response 作比较，如果相同表明验证通过，如果不相同表明验证失败。

联想网络的认证计费解决方案采用的是 EAP 用户验证方法。

8.3 配置 802.1x

本节对 802.1x 的配置进行详细的描述，主要包括以下内容：

- 802.1x 缺省配置
- 启动和关闭 802.1x
- 配置 802.1x 端口状态
- 配置重新认证机制
- 配置端口接入主机最大个数
- 配置间隔时间和重发次数
- 显示 802.1x 信息

1. 802.1x缺省配置

iSpirit 3626 交换机 802.1x 配置缺省情况如下：

802.1x 是关闭的。

所有端口的状态是 N/A。

重新认证机制是关闭的，重新认证的间隔时间是 3600 秒。

所有端口的接入主机最大个数是 9 个。

重发 EAP-Request 的超时间隔为 30 秒。

超时重发 EAP-Request 的次数为 3 次。

用户认证失败等待的时间为 60 秒。

服务端超时重发的时间间隔为 10 秒。

交换机在全局 CONFIG 模式下提供一个命令让所有的配置回到缺省状态，命令如下：

dot1x default

2．启动和关闭802.1x

● 配置 802.1x 的第一步是启动 802.1x。在全局 CONFIG 模式下输入下面的命令启动 802.1x：

dot1x

● 当关闭 802.1x 时，所有的端口状态回到 N/A 状态。在全局 CONFIG 模式下输入下面的命令关闭 802.1x：

no dot1x

3.配置802.1x端口状态

在设置 802.1x 端口状态前一定要启动 802.1x。如果端口下的所有的用户必须通过认证后才能访问网络，则该端口必须设置成 Auto 状态。

● 下面的命令在全局 CONFIG 模式下设置端口为 Auto 状态：

dot1x control auto {<port>|<port1-port2>} [<port>|<port1-port2>] …

● 下面的命令在 PORT RANGE 模式下设置端口为 Auto 状态：

dot1x control auto

● 下面的命令在全局 CONFIG 模式下设置端口为 Force-authorized 状态：

dot1x control force-authorized {<port>|<port1-port2>} [<port>|<port1-port2>] …

● 下面的命令在 PORT RANGE 模式下设置端口为 Force-authorized 状态：

dot1x control force-authorized

● 下面的命令在全局 CONFIG 模式下设置端口为 Force-unauthorized 状态：

dot1x control force-unauthorized {<port>|<port1-port2>} [<port>|<port1-port2>] …

● 下面的命令在 PORT RANGE 模式下设置端口为 Force-unauthorized 状态：

dot1x control force-unauthorized

● 下面的命令在全局 CONFIG 模式下设置端口为 N/A 状态：

no dot1x control {<port>|<port1-port2>} [<port-|<port1-port2>] …

● 下面的命令在 PORT RANGE 模式下设置端口为 N/A 状态：

no dot1x control

注意：

如果一个端口已经绑定了 MAC 地址，那么这个端口不能设置为 Auto、Force-authorized 或 Force-unauthorized 状态。

4.配置重新认证机制

为了防止客户端异常下线后交换机和认证服务器无法察觉，iSpirit 3626 交换机提供了重新认证机制，每隔重新认证间隔时间交换机发起一次认证。

● 下面的命令在全局 CONFIG 模式下启动重新认证机制：

dot1x reauthenticate

● 下面的命令在全局 CONFIG 模式下关闭重新认证机制：

no dot1x reauthenticate

- 下面的命令在全局 CONFIG 模式下设置重新认证的间隔时间：

  dot1x timeout re-authperiod <interval>

  注意：

  重新认证的间隔时间不要设置太短，否则网络带宽以及交换机的 CPU 资源消耗太大。

5.配置端口接入主机最大个数

iSpirit 3626 交换机的每个端口都可控制接入的最大主机个数，此功能可以限制用户使用多台主机非法接入到网络中。端口接入主机最大个数缺省是 100 个，最大可以设置成 100 个。如果端口的接入主机最大个数设置为 0，那么该端口拒绝任何用户接入。

下面的命令在全局 PORT RANGE 模式下设置端口接入主机最大个数：

dot1x support-host <number>

6.配置间隔时间和重发次数

802.1x 协议标准中规定了协议交互和协议状态机的一些间隔时间和重发次数，iSpirit 3626 交换机使用了标准的间隔时间和重发次数，建议用户在使用时不要改这些间隔时间和重发次数。

tx-period 表示交换机重发 EAP-Request 协议包的间隔时间；max-req 表示交换机重发 EAP-Request 的次数；quiet-period 表示用户认证失败时等待用于重新认证的间隔时间；server-timeout 表示交换机给认证服务器重发 RADIUS 包的间隔时间。

下面的命令在全局 CONFIG 模式下配置这些间隔时间和重发次数：

dot1x timeout tx-period <interval>

dot1x max-req <number>

dot1x timeout quiet-period <interval>

dot1x timeout server-timeout <interval>

7.显示802.1x信息

下面的命令在全局 CONFIG 模式或 PORT RANGE 模式下显示 802.1x 的信息，当不输入端口参数，显示所有的 802.1x 配置信息，包括所有端口的配置信息，当输入端口参数，显示该端口下的所有接入用户的信息：

show dot1x [m/p]

8.4 配置 RADIUS

本节对 RADIUS 的配置进行详细的描述，主要包括以下内容：

- RADIUS 缺省配置
- 配置认证服务器的 IP 地址
- 配置共享密钥
- 启动和关闭计费
- 配置 RADIUS 端口和属性信息
- 显示 RADIUS 信息

1.RADIUS缺省配置

iSpirit 3626 交换机 RADIUS 配置缺省情况如下：

没有配置主认证服务器和备份认证服务器的 IP 地址，也就是 IP 地址是 0.0.0.0。

没有配置共享密钥，也就是共享密钥字符串为空。

计费缺省是启动的。

RADIUS 认证 UDP 端口为 1812，计费 UDP 端口为 1813。

RADIUS 属性 NASPort 的值为 0xc353，NASPortType 的值为 0x0f，NASPortServer 的值为 0x02。

2.配置认证服务器的IP地址

为了使交换机与认证服务器之间进行 RADIUS 通信，在交换机上需要配置认证服务器的 IP 地址。在实际应用中，可以使用一台认证服务器，也可以使用两台认证服务器，一台作为主认证服务器，一台作为备份认证服务器。如果交换机配置了两台认证服务器的 IP 地址，当交换机与主认证服务器中断通信后可以切换到与备份认证服务器通信。

- 下面的命令在全局 CONFIG 模式下配置主认证服务器的 IP 地址：

  radius-server host <ip-address>

- 下面的命令在全局 CONFIG 模式下配置备份认证服务器的 IP 地址：

  radius-server option-host <ip-address>

3.配置共享密钥

交换机和认证服务器之间要相互鉴权，交换机和认证服务器上都需要设置一个相同的共享密钥。注意交换机上的共享密钥一定要和认证服务器的相同。

下面的命令在全局 CONFIG 模式下配置交换机的共享密钥：

radius-server key <string>

4.启动和关闭计费

如果交换机关闭了计费，交换机在认证成功后或用户下线时不会给认证服务器发 RADIUS 计费包。一般在实际应用时，计费是打开的。

- 下面的命令在全局 CONFIG 模式下启动计费：

  radius-server accounting

- 下面的命令在全局 CONFIG 模式下关闭计费：

  no radius-server accounting

5.配置RADIUS端口和属性信息

建议用户不要修改 RADIUS 端口和属性信息配置。

- 下面的命令在全局 CONFIG 模式下修改 RADIUS 认证 UDP 端口：

  radius-server udp-port <port-number>

- 下面的命令在全局 CONFIG 模式下修改 RADIUS 属性信息：

  radius-server attribute nas-portnum <number>

  radius-server attribute nas-porttype <number>

radius-server attribute service-type <number>

6.显示RADIUS信息

下面的命令在全局 CONFIG 模式下显示 RADIUS 配置信息：

show radius-server

第 9 章 配置 MAC 绑定

在实际的网络中，用户的接入安全是管理员非常关注的问题。iSpirit 3626 交换机提供了多种方式实现了用户的接入安全，其中就包括 MAC 绑定方式。本章介绍如何配置 MAC 绑定功能，主要包括以下内容：

1、MAC 绑定介绍

2、MAC 绑定配置

3、MAC 绑定配置示例

9.1 MAC 绑定介绍

MAC 绑定可以实现网络中的用户的接入安全。用户是通过交换机的端口接入到网络。如果交换机中的某端口绑定了特定的 MAC 地址，那么这些特定的 MAC 地址就是合法的 MAC 地址，交换机允许这些合法的 MAC 地址的用户从该端口接入网络，不允许非法的 MAC 地址的用户接入网络，实现用户的接入安全。

如果交换机的某端口绑定了 MAC 地址，交换机会一直检查从该端口输入的数据流，如果数据流的源 MAC 地址是被绑定的合法的 MAC 地址，该数据流允许转发，如果数据流的源 MAC 地址不是被绑定的合法的 MAC 地址，该数据流丢弃。通过丢弃输入的数据流来防止非法用户接入网络。

IEEE802.1Q 标准支持 SVL 和 IVL 两种 MAC 地址学习模式。SVL 指 MAC 地址与 VLAN 没有关系，在所有的 VLAN 中 MAC 地址必须唯一，在学习 MAC 地址时不关心 VLAN。IVL 指 MAC 地址与 VLAN 有关系，在不同的 VLAN 中 MAC 地址可以相同，但在一个 VLAN 内 MAC 地址必须唯一，在学习 MAC 地址时必须知道该 MAC 地址所属的 VLAN。iSpirit 3626 交换机支持 IVL 模式，在做 MAC 绑定时必须指定这些 MAC 地址所属的 VLAN。

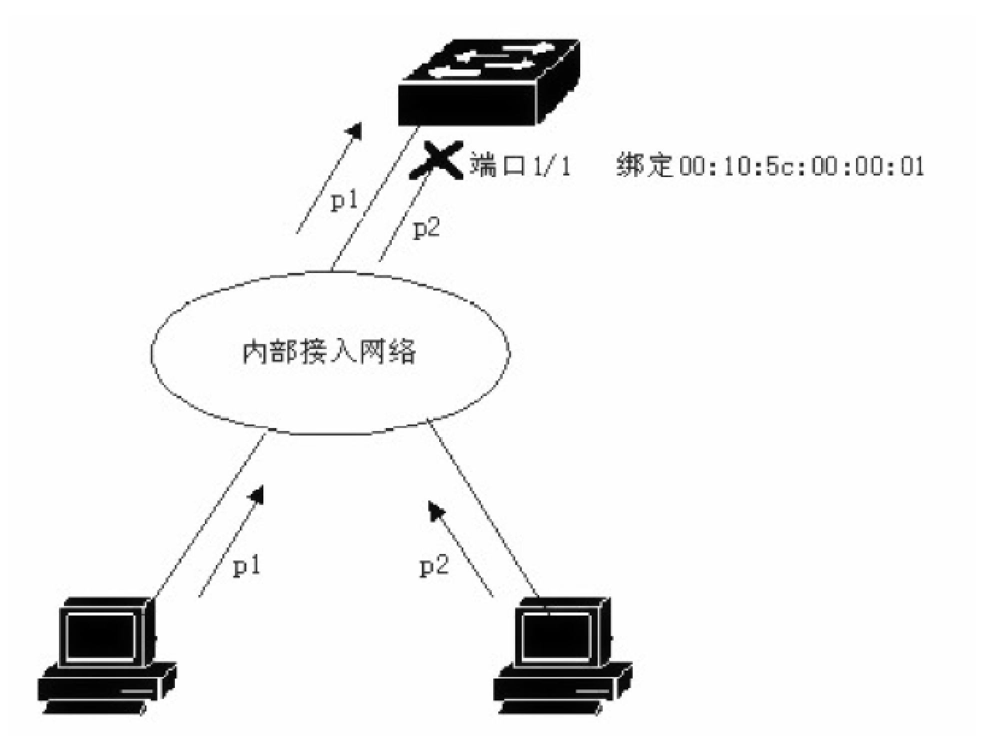


图 9-1 用户从绑定的端口接入网络

图 9-1 是一个 MAC 绑定的例子，iSpirit 3626 交换机的端口 1 绑定了 MAC 地址 00:10:5C:00:00:01，在该端口下，有两个用户想从该端口接入网络，用户 1 的 MAC 地址是 00:10:5C:00:00:01，用户 2 的 MAC 地址是 00:10:5C:00:00:02。用户 1、用户 2 和交换机的端口 1 属于一个子网。只有用户 1 可以通过交换机的端口 1 接入网络，用户 2 不能通过交换机的端口 1 接入网络。用户 1 发出来的数据流 p1 可以通过交换机的端口 1 转发，而用户 2 发出来的数据流 p2 则在交换机的端口 1 处丢弃。

当交换机的某端口绑定了 MAC 地址时，这些 MAC 地址只能通过此交换机的该端口访问网络，不能通过该交换机的其它端口访问网络。交换机的不同端口不能绑定相同的 VLAN 的相同的 MAC 地址。如果一个端口 A 绑定了一个 MAC 地址，另一个端口 B 没有绑定 MAC 地址，端口 A 和 B 在同一个 VLAN，则拥有该 MAC 地址的用户不能通过交换机的端口 B 访问网络。如图 1 假设交换机的端口 1 绑定了 MAC 地址 00:10:5C:00:00:01，端口 2 没有绑定 MAC 地址，端口 1 和 2 属于同一个 VLAN，则用户 1 不能通过交换机的端口 2 访问网络，只能通过交换机的端口 1 访问网络。

当一个端口绑定了一个或多个 MAC 地址时，不会影响从这个端口输入的数据流的转发效率，数据流可以实现线速转发。一个端口最多可以绑定 128 个 MAC 地址。

端口绑定 MAC 地址与 802.1x 端口状态是互斥的。如果一个端口的 802.1x 状态已经设置为 Auto、Force-authorized 或 Force-unauthorized，那么这个端口不能绑定 MAC 地址。

9.2 MAC 绑定配置

iSpirit 3626 交换机支持手工绑定 MAC 地址和自动绑定 MAC 地址。手工绑定 MAC 地址是用户通过命令一个一个输入 MAC 地址与端口进行绑定。自动绑定 MAC 地址是把二层硬件转发表中该端口的已有的条目读出来直接进行 MAC

地址绑定。

如果一个端口已经绑定了 MAC 地址，此时自动绑定 MAC 地址无效，只能进行手工绑定 MAC 地址。自动绑定 MAC 地址只能在端口没有绑定 MAC 地址时进行。如果二层硬件转发表中该端口没有条目，自动绑定 MAC 地址无效，此时端口没有绑定任何 MAC 地址。如果二层硬件转发表中该端口的条目超过了 128 个，自动绑定 MAC 地址时只有前 128 个进行绑定。

iSpirit 3626 交换机缺省情况任何一个端口都没有绑定 MAC 地址。

● 下面的命令在全局 CONFIG 模式下一个端口绑定 MAC 地址。如果不输入 vlanid 和 mac-address 参数，此时进行自动绑定 MAC 地址，把硬件转发表中相关的条目进行绑定 MAC 地址。如果输入 vlanid 和 mac-address 参数，进行手工绑定一个 MAC 地址，如果要手工绑定多个 MAC 地址，需要重复此命令：

mac bind <port> [<vlanid> <mac-address>]

注意：

如果进行自动绑定 MAC 地址，MAC 地址绑定无效或失败的原因可能如下：

该端口的 802.1x 状态已经设置为 Auto、Force-authorized 或 Force-unauthorized。

该端口已经绑定了 MAC 地址。

二层硬件转发表中该端口没有条目。

如果进行手工绑定 MAC 地址，MAC 地址绑定无效或失败的原因可能如下：

该端口的 802.1x 状态已经设置为 auto、Force-authorized 或 Force-unauthorized。

该端口已经绑定了 VLAN 和 MAC 地址都相同的条目。

该端口已经绑定了 128 个 MAC 地址。

● 下面的命令在全局 CONFIG 模式下解除一个端口的 MAC 地址绑定。如果不输入 vlanid 和 mac-address 参数，解除该端口下的所有 MAC 地址绑定。如果输入 vlanid 和 mac-address 参数，解除该端口下的一个指定的 MAC 地址绑定：

no mac bind <port> [<vlanid> <mac-address>]

● 下面的命令在全局 CONFIG 模式下显示 MAC 地址绑定信息。如果不输入 port 参数，显示所有的端口的 MAC 地址绑定信息。如果输入 port 参数，显示指定的端口的 MAC 地址绑定信息：

show mac bind [port]

第 10 章 配置 IP 绑定

在实际的网络中，用户的接入安全是管理员非常关注的问题。iSpirit 3626 交换机提供了多种方式实现了用户的接入安全，其中就包括 IP 绑定方式。

本章介绍如何配置 IP 绑定功能，主要包括以下内容：

1、IP 绑定介绍

2、IP 绑定配置

3、IP 绑定配置示例

10.1 IP 绑定介绍

IP 绑定可以实现网络中的用户的接入安全。用户是通过交换机的端口接入到网络。如果交换机中的某端口绑定了特定的 IP 地址，那么这些特定的 IP 地址就是合法的 IP 地址，交换机允许这些合法的 IP 地址的用户从该端口接入网络，不允许非法的 IP 地址的用户接入网络，实现用户的接入安全。

如果交换机的某端口绑定了 IP 地址，交换机会一直检查从该端口输入的数据流，如果数据流的源 IP 地址是被绑定的合法的 IP 地址，该数据流允许转发，如果数据流的源 IP 地址不是被绑定的合法的 IP 地址，该数据流丢弃。通过丢弃输入的数据流来防止非法用户接入网络。

图 10-1 是一个 IP 绑定的例子，iSpirit 3626 交换机的端口 1 绑定了 IP 地址 192.168.0.100，在该端口下，有两个用户想从该端口接入网络，用户 1 的 IP 地址是 192.168.0.100，用户 2 的 IP 地址是 192.168.0.101。只有用户 1 可以通过交换机的端口 1 接入网络，用户 2 不能通过交换机的端口 1 接入网络。用户 1 发出来的数据流 p1 可以通过交换机的端口 1 转发，而用户 2 发出来的数据流 p2 则在交换机的端口 1 处丢弃。

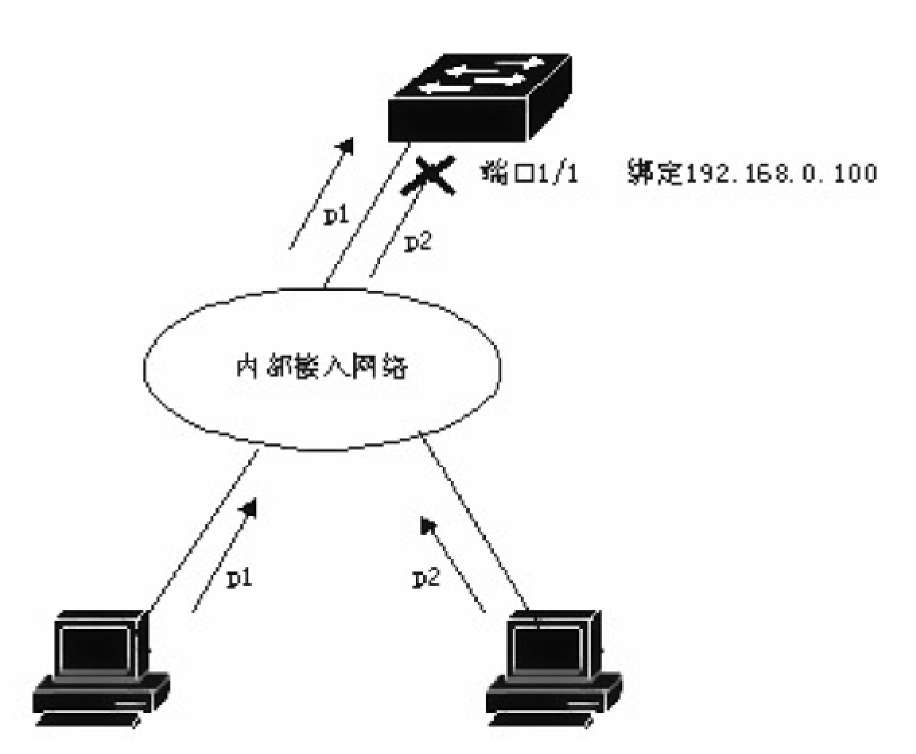


图 10-1 用户从绑定的端口接入网络

IP 绑定只控制交换机的端口的接入安全。交换机的不同端口可以绑定相同的 IP 地址。如果一个端口 A 绑定了一个 IP 地址，另一个端口 B 没有绑定 IP 地址，拥有该 IP 地址的用户可以通过交换机的端口 B 访问网络。如图 1 假设交换机的端口 1 绑定了 IP 地址 192.168.0.100，端口 2 没有绑定 IP 地址，则用户 1 也可以从交换机的端口 2 访问网络。

交换机通过端口的 FFP 实现 IP 地址的绑定，不影响绑定的 IP 地址的数据流的转发效率，数据流可以实现线速转发。因为每个端口 FFP 的容量有限，所以一个端口绑定的 IP 地址个数也是有限的。一个端口最多可以绑定 127 个 IP 地址，如果 FFP 被其它应用占用，一个端口绑定的 IP 地址个数会更少。

IP 绑定与 ACL 过滤、QoS 的非信任端口是互斥的。如果一个端口已经做了 ACL 过滤，则该端口不能做 IP 绑定。如果一个端口是 QoS 的非信任端口，则该端口也不能做 IP 绑定。

如果一个端口能做 IP 地址绑定不能绑定到 127 个 IP 地址，此时说明其它的应用占用了 FFP 资源，占用该端口的 FFP 资源的应用可能是 QoS 信任端口、IGMP SNOOPING 协议和 802.1x 协议。

10.2 IP 绑定配置

iSpirit 3626 交换机只支持手工绑定 IP 地址，也就是说一个端口绑定的一个或多个 IP 地址都是用户手工输入的。

iSpirit 3626 交换机缺省情况下任何一个端口都没有绑定 IP 地址。

下面的命令在全局 CONFIG 模式下一个端口绑定一个 IP 地址，如果一个端口需要绑定多个地址，要重复输入此命令：

ip bind <port> <ip-address>

注意：

如果在输入命令之前该端口没有绑定 IP 地址，此命令失败的可能原因是：

1.该端口已经做了 ACL 过滤。

2.该端口已经是 QoS 非信任端口。

如果在输入命令之前该端口已经绑定了 IP 地址，此命令失败的可能原因是：

1.该 IP 地址已经与该端口绑定了。

2.FFP 资源不够，可能该端口是 QoS 信任端口或（和）IGMP SNOOPING 协议启动了或（和）该端口处于 802.1x 的 Auto 模式。

● 下面的命令在全局 CONFIG 模式下解除一个端口的 IP 地址绑定，如果不输入 ip-address 参数，则解除该端口的所有 IP 地址的绑定，如果输入 ip-address 参数，则解除该端口的一个指定的 IP 地址的绑定：

no ip bind <port> [ip-address]

● 下面的命令在全局 CONFIG 模式下显示 IP 地址绑定的信息，如果不输入 port 参数，显示所有的端口的 IP 地址绑定信息，如果输入 port 参数，显示指定的端口的 IP 地址绑定信息：

show ip bind [port]

第 11 章 配置 ACL

在实际的网络中，网络的访问安全是管理员非常关注的问题。iSpirit 3626 交换机支持 ACL 过滤提供网络的访问安全。通过配置 ACL 规则，交换机根据这些规则对输入的数据流过滤实现网络的访问安全。本章介绍如何配置 ACL，主要包括以下内容：

1、ACL 资源库介绍

2、ACL 过滤介绍

3、ACL 资源库配置

4、ACL 过滤配置

5、ACL 配置示例

11.1 ACL 资源库介绍

ACL(Access list control)资源库是多组访问规则的集合，ACL 资源库不具备控制数据的转发功能，只是一个具有冲突排序的规则集合。ACL 资源库在被应用引用后，可以控制经过交换机的数据包的转发；应用通过规则的 deny 或 permit 来控制通过设备的数据包。ACL 可以应用于端口访问过滤，服务访问过滤和 QOS。

ACL 资源库有标准 IP 规则组（组号 1～199），扩展 IP 规则组（组号 200～399），扩展 MAC 规则组（组号 400~599），一共 599 组；每一组规则支持 128 条规则。每一组规则内部自动进行冲突规则优先顺序排序。

在应用时，当一个数据包通过一个端口的时候，交换机将每一条规则中的字段和数据包中相应的所有字段进行比较；当同时出现多个规则完全匹配时，最后一条完全匹配的规则生效；由最后一条匹配的规则来决定数据包是转发还是丢弃。所谓的完全匹配是，规则中的字段的值和数据包中相应字段的值完全相等。只有完全匹配 ACL 某一条规则，这规则才会作相应的 deny 或 permit 操作。

在 iSpirit 3626 中，同一组内的规则是自动排序的。规则的自动排序相对比较复杂，在排序过程中’范围’大的规则排在前面，’范围’小的排在后面。范围的大小由规则的约束条件决定；规则的约束条件越少’范围’就越大，规则的约束条件越多’范围’就越小。规则的约束条件主要体现在地址的 wildcard 和一些非地址字段的个数两方面。Wildcard 是 bit 串。IP 地址是四字节，MAC 地址是六字节。bits 为’1’表示不需要匹配，bits 为’0’表示要匹配。非地址字段是指 vlanId，协议类型，IP 协议类型，协议端口，这些字段也隐藏了一个 wildcard。他们的长度是相应字段的字节长度，因此相同的字段长度是统一的，只需计算字段的个数。Wildcard 为’0’的 bit 越多约束条件就越多。

下面以端口访问过滤为例说明规则排序的必要性和自动排序的优点。假如用户需要拒绝源地址为 192.168.0.0/16 网段的地址转发，允许源地址为 192.168.1.0/24 网段的地址转发，可以配置以下两条规则：

access-list 1 deny 192.168.0.0 0.0.255.255－**规则 1**

access-list 1 permit 192.168.1.0 0.0.0.255 －**规则 2**

后面简称规则 1 和规则 2。

这两条规则是有冲突的；因为**规则 2** 的地址包含在**规则 1 的**地址中，而且一个是 deny，一个是 permit；根据 ACL 的过滤原理，不同的顺序有不同的结果。如果要实现上述要求，上面两条规则的顺序必须是：**规则 1** 排在前面，**规则 2** 排在后面。iSpirit 3626 自动实现了上述的排序功能，无论用户以怎样的先后顺序配置上述的规则，最后的顺序都是**规则 1** 排在**规则 2** 的前面。当一个源地址为 192.168.1.1 地址的包上来转发时，首先比较第一条规则，再往后进行比较第二条规则，两条规则都匹配，后面的生效(转发)；如果源地址为 192.168.0.1 时,只有第一条匹配，那么就丢弃(不

转发)。如果没有进行排序，用户可能会现先配置规则**规则 2**，后配置**规则 1**；**规则 1** 排在后面，**规则 2** 排在前面。

access-list 1 permit 192.168.1.0 0.0.0.255 －**规则 2**

access-list 1 deny 192.168.0.0 0.0.255.255－**规则 1**

因为后面的**规则 1** 包含了前面的**规则 2**，会导致的情况是：完全匹配**规则 2** 的数据包也完全匹配**规则 1**，**规则 1** 每次都会生效；而不能达到应用的需求。

在 iSpirit 3626 中，'0.0.255.255'是 Wildcard bits，bits 为'1'表示不需要匹配，bits 为'0'表示要匹配。由此可以看出**规则 1** 的 Wildcard bits 为'0.0.255.255'，需要匹配两个字节(16 个 bits)；**规则 2** 中，的 Wildcard bits 为'0 0.0.0.255'，需要匹配三个字节(24 个 bits)；所以**规则 1** 的规则'范围'更大，因此排在前面。在扩展 IP 中，排序需要考虑更多的规则字段，如 IP 协议类型,通信端口等等。它们的排序规则是一样的，即配置限制越多规则的'范围'就越小，反之'范围'就越大。规则的排序在后台实现，用户命令只能按用户配置的先后顺序显示。

ACL 支持的过滤字段包括了源 MAC 地址，目的 MAC 地址，VLANID，协议类型(如：IP,ARP)，源 IP，目的 IP，IP 协议类型(如：TCP，UDP，OSPF)，源端口（如 161），目的端口。用户可以根据不同的需要，配置不同的规则来进行访问控制。

在 iSpirit 3626 中，一组规则可以被多个应用所应用；如：一组规则被端口访问过滤和服务访问过滤同时引用或同时被两个端口的端口访问过滤所引用。只要一组规则被某一个或多个应用所引用，就不能对这一组规则添加，修改或删除操作；只有在这一组规则不被引用时才能进行这些操作。在执行 show access-list 命令时会显示这一组被引用的计数。

在每一组的 ACL 规则中，缺省隐藏一条的拒绝所有 IP 协议（0x0800）包的规则。但是如果规则中有存在一条拒绝或允许所有 IP 协议（0x0800）包的规则，这条隐藏的规则便不会存在。

11.2 ACL 过滤介绍

ACL 过滤是在交换机的输入端口处进行的，对输入到此端口的数据流进行规则匹配实现端口的过滤。ACL 过滤都是交换机的硬件进行处理的，不会影响数据流的转发效率。

当交换机的某端口没有配置 ACL 过滤时，所有通过该端口输入的数据流不会进行规则匹配，可以通过该端口进行转发。当交换机的某端口配置了 ACL 过滤时，所有通过该端口的输入数据流会进行规则匹配，匹配的规则的动作如果是 permit，该数据流允许转发，如果是 deny，该数据流不允许转发，丢弃。

在配置端口的 ACL 过滤时，一个端口只能选择一个 ACL 规则组，选择后该组规则导入到端口的 FFP 中，如果该组规则中没有拒绝或允许所有 IP 协议（0x0800）包的规则，则写入 FFP 时会加一条拒绝所有 IP 协议（0x0800）的规则。

例如一组规则中只有一条规则：access-list 1 permit 192.168.1.0 0.0.0.255，缺省会隐藏一条拒绝所有 IP 协议（0x0800）包的规则，实际上会有两条规则导入到端口的 FFP。在数据流过滤时，只有源地址从 192.168.1.0 到 192.168.1.255 的数据流可以通过该端口进行转发，所有其它的数据流被过滤掉。

例如一组规则中有两条规则：access-list 1 deny 192.168.1.0 0.0.0.255 和 access-list 1 permit any。此时有一条允许所有 IP 协议（0x0800）包的规则，这时不存在隐藏的规则，实际上会有两条规则导入到端口的 FFP。在数据流过滤时，只有源地址从 192.168.1.0 到 192.168.1.255 的数据流被过滤掉，所有其它的数据流被可以进行转发。

如图 11-1 是一个 ACL 过滤的例子。iSpirit 3626 交换机的端口 1 选择一个 ACL 规则组 1，该组规则中只有一条规则 access-list 1 permit 192.168.0.100。在交换机的端口 1 下，有两个用户想从该端口接入网络，用户 1 的 IP 地址是 192.168.0.100，用户 2 的 IP 地址是 192.168.0.101。只有用户 1 可以通过交换机的端口 1 接入网络，用户 2 不能通

过交换机的端口 1 接入网络。用户 1 发出来的数据流 p1 可以通过交换机的端口 1 转发，而用户 2 发出来的数据流 p2 则在交换机的端口 1 处丢弃。

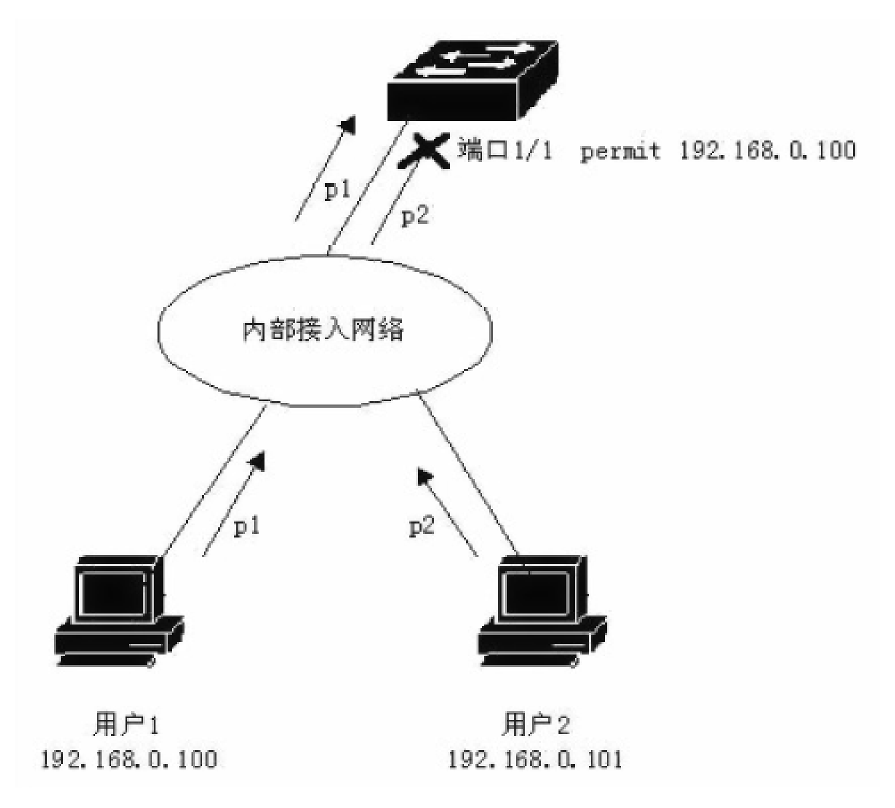


图 11-1　用户从 ACL 过滤的端口接入网络

ACL 过滤与 IP 绑定是互斥的，如果一个端口已经做了 IP 绑定，则该端口不能做 ACL 过滤。ACL 过滤与 QoS 非信任端口的配置有一定的顺序，端口必须先配置 ACL 过滤，后配置 QoS 非信任端口。如果一个端口已经配置为 QoS 非信任端口，此时该端口不能配置 ACL 过滤，必须先清除 QoS 配置后再做 ACL 过滤。

ACL 过滤需要使用端口的 FFP 资源，当端口配置 ACL 过滤失败时，有可能是 FFP 资源不足，但 ACL 组中的规则太多所致，此时可能被 QoS 等其它应用占用了 FFP 资源。

多个端口做 ACL 过滤时可以选用同一个 ACL 规则组，使用相同的过滤规则。一个端口在做 ACL 过滤和 QoS 非信任端口时可以选用相同的规则。

11.3 ACL 资源库配置

iSpirit 3626 交换机缺省没有任何规则。

在 iSpirit 3626 中的资源库支持三类 ACL 规则：标准 IP 规则，扩展 IP 规则，扩展 MAC 规则。下面分三类规则来介绍 ACL 的配置。

- **标准 IP 规则**：标准 IP 规则是通过源 IP 地址来控制数据包的转发。

命令形式：access-list <groupId> {deny|permit} <source>

参数说明：

groupId：访问控制列表组号，标准 IP ACL 支持从 1 到 199 组。规则号是顺序递增的，由系统自动产生。

deny/permit：如果完全匹配，则拒绝或允许该数据包转发。

source：源 IP 有三种输入方式：

A.B.C.D wildcard 可以控制来自一个网段的 IP 地址；

any 相当于 A.B.C.D 255.255.255.255

host A.B.C.D 相当于 A.B.C.D 0.0.0.0

wildcard：决定哪些 bits 需要匹配，'0'表示需要匹配，'1'表示不需要匹配。

● **扩展 IP 规则**：扩展 IP 规则是标准 IP 规则的扩展，可以通过源 IP，目的 IP，IP 协议类型和服务端口来控制数据包的转发。

命令形式：access-list <groupId>{deny|permit}<protocol><source> [eq srcPort] {destination}[destPort]

参数说明：

groupId：访问控制列表组号，扩展 IP ACL 支持从 200 到 399 组。规则号是顺序递增的，由系统自动产生。

deny/permit：如果完全匹配，则拒绝或允许该数据包转发。

protocol：在 IP 层之上的协议类型，如：icmp，tcp，udp 等，也可以输入相应的数字 6(tcp)。如果不需要对这些协议进行控制，可以输入 ip 或(0)。

source：源 IP 有三种输入方式：

1)A.B.C.D wildcard 可以控制来自一个网段的 IP 地址；

2)any 相当于 A.B.C.D 255.255.255.255

3)host A.B.C.D 相当于 A.B.C.D 0.0.0.0

srcPort：是对于 protocol 为 tcp 或 udp 的情况，可以控制数据包的源端口，输入方式可以是一些熟悉的端口服务名称，如：www、也可以是数字，如 80。

destination：目的 IP 有三种输入方式：

1) A.B.C.D wildcard 可以控制来自一个网段的 IP 地址；

2) any 相当于 A.B.C.D 255.255.255.255

3) host A.B.C.D 相当于 A.B.C.D 0.0.0.0

destPort：是对于 protocol 为 tcp 或 udp 的情况，可以控制数据包的目的端口，输入方式和 srcPort 相同。

● **扩展 Mac 规则**：扩展 mac 规则是通过源 mac 地址，目的 mac 地址，vlanId 和协议类型来控制数据包的转发。

命令形式：access-list <groupId> {deny|permit} <vlanId> <type> <source> <destination>

参数说明：

groupId：访问控制列表组号，扩展 MAC ACL 支持从 400 到 599 组。规则号是顺序递增的，由系统自动产生。

deny/permit：如果完全匹配，则拒绝或允许该数据包转发。

vlanId: 配置数据包来自哪个 vlan，如果不需要匹配这一项可以输入 0。

type：type 只协议类型，如 ip，arp，rarp 等，也可以输入十六进制数字如 0806(ip)。

Source：源 IP 有两种种输入方式：

1)AA:BB:CC:DD:EE:FF wildcard，可以控制一些 MAC 地址的网段(类似 IP 地址)

2)any 相当于 AA:BB:CC:DD:EE:FF FF:FF:FF:FF:FF:FF

destination：目的 IP 有两种种输入方式：

1)AA:BB:CC:DD:EE:FF wildcard，可以控制一些 MAC 地址的网段(类似 IP 地址)

2)any 相当于 AA:BB:CC:DD:EE:FF FF:FF:FF:FF:FF:FF

其他命令列表：

show access-list [groupId]

显示当前 ACL 中配置的规则列表。如果输入了 groupId 则当前组的规则列表；否则显示所有的规则列表。

no access-list <groupId> [ruleId]

删除指定的规则列表。如果输入了 ruleId，则删除组中指定的规则；否则删除 groupId 组的所有规则。删除规则可能失败，可能原因是这条规则被其他应用所引用。

11.4 ACL 过滤配置

iSpirit 3626 交换机缺省所有的端口都没有做 ACL 过滤。

命令列表：

1.acl-filter <groupId>

模式：PORT CONFIGURATION

参数：

groupId：和端口绑定的 ACL 组号

功能：配置 ACL 端口过滤。

注意：

如果上面的命令配置失败或无效，可能有下面的原因：

规则组 groupId 不存在或存在但状态不是 active。

该端口已经做了 ACL 过滤。

该端口已经做了 IP 绑定。

该端口已经是 QoS 非信任端口。

ACL 组中的规则太多或 FFP 被 QoS 等其它应用占用。

2.Show acl-filter [port]

模式：PORT CONFIGURATION/CONFIGURATION

参数：

M/P：可选项，输入只显示当前端口相关的 ACL 组，没有输入显示所以端口相关的 ACL 组。

功能：显示 ACL 端口过滤配置；

3.no acl-filter <groupId>

模式：PORT CONFIGURATION

参数：

groupId：和端口绑定的 ACL 组号

功能：删除当前端口和 ACL 端口过滤相关的配置。

第 12 章 配置 QoS

本章主要包括以下内容：

1、QoS 介绍

2、QoS 配置

3、QoS 配置示例

本章描述如何通过 QoS 命令来配置 iSpirit 3626 交换机的 QoS 服务。

当交换机没有配置 QoS 时，交换机使用同一个优先级转发所有通过交换机的数据流，不能保证数据流的可靠性、延时和吞吐量。

有些应用需要低延时，有些应用需要高可靠性，而有些应用则需要有稳定的吞吐量，这时就需要启动交换机的 QoS 功能，交换机可以对不同的数据流进行不同的优先级处理。

注意：

如果您需要 QoS 命令的详细信息，请参见命令参考。

12.1 QoS 介绍

iSpirit 3626 交换机实现了强大的 QoS 功能。使用交换机的 QoS 功能，您能够让通过交换机转发的重要的数据流得到优先的处理，并对一些数据流进行带宽限制，使您的网络的带宽利用更加合理，网络性能变得可预测。

iSpirit 3626 交换机实现了基于 IETF 标准的 DiffServ 体系结构的 QoS 功能，在 QoS 域的边界对数据流进行分类，给每个数据流打上一个 DSCP 值，在 QoS 域内根据数据流的 DSCP 值进行优先级处理。iSpirit 3626 交换机不仅实现了 DiffServ 的 QoS，还实现了 802.1p 的 QoS 以及早期应用的比较多的 IP Precedence 的 QoS。

不同的 QoS 使用不同的优先级标记，下面分别介绍三种 QoS 的标记：

802.1p的QoS

802.1p 的 QoS 使用以太网帧中的 2 个字节的 TAG 标记中的最高三位作为其优先级，如图 1 所示。优先级的范围从 0 到 7。如果在 QoS 域中使用 802.1p 的 QoS，需要所有的数据包在网络上传输时都有 TAG 标记，比较适合在一个小范围的局域网中使用。

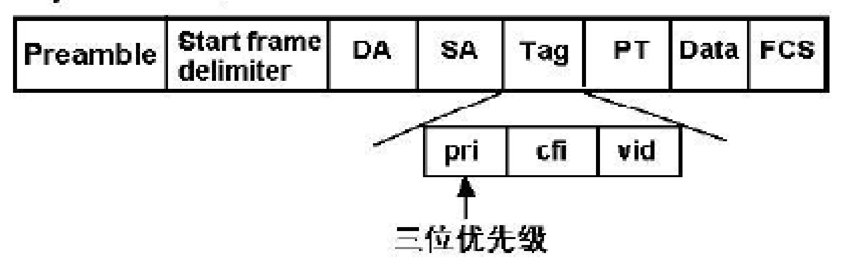


图 12-1　802.1p 的优先级位

IP Precedence的QoS

IP Precedence 的 QoS 使用 IP 数据包头的 TOS 字段的最高三位作为其优先级，如图 2 所示。IP Precedence 的范围从 0 到 7。IP Precedence 的 QoS 在早期使用比较多，现在逐渐被 DiffServ 取代。

DiffServ的QoS

DiffServ 的 QoS 使用 DSCP 作为其优先级标记，DSCP 位于 IP 数据包头的 TOS 字段的最高六位，如图 2 所示。DSCP 的范围从 0 到 63。

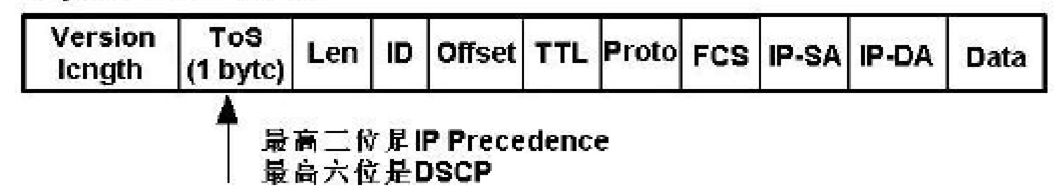


图 12-2　IP Precedence 和 DiffServ 的优先级位

在 QoS 域的边界，根据交换机的 QoS 配置策略把不同的数据流打上不同的优先级标记，也就是业务类标记，在 QoS 域内所有的设备根据业务类标记对数据流进行转发。这样，QoS 域内的设备不需要执行复杂的流分类和复杂的 QoS 策略，只需要使用业务类标记进行优先级处理。

当数据流进入 QoS 域的边界，QoS 域边界的交换机不仅会把数据流归并到业务类中，还可以对业务类进行带宽处理，比如进行带宽资源的预留或做带宽的限制，这样可以保证 QoS 域中的带宽资源得到合理的利用。

为了保证网络中端到端的服务质量保证，在 QoS 域中的所有设备都需要具有相应的 QoS 功能。QoS 域边界的交换机需要具有强大的 QoS 功能，能够根据 IP 数据包的多个字段对数据流进行分类，能够根据业务类进行带宽分配，能够支持多种调度策略。QoS 域内的交换机只需要根据业务类标记进行优先级处理就行了。iSpirit 3626 能够作为域边界交换机，也能够作为域内交换机。

本节主要包括以下几部分内容：

- 常见术语
- QoS 模型
- 业务分类
- QoS 策略
- QoS 调度
- FFP 简介

● 常见术语

QoS 域：一些网络和设备的集合，在域中所有的设备采用相同的 QoS 策略，实现端到端的服务质量保证。

业务类（class）：在一个 QoS 域内采用相同的 QoS 策略的数据流的集合，可以包括一个数据流，也可以包括多个数据流。

业务类标记（class information）：标识一个业务类，可以是 COS 值、IP Precedence 值和 DSCP 值。

COS：802.1p 的业务类标记，值范围从 0 到 7，每个值标识一个业务类型。

IP Precedence：早期 IP 网络使用的一种业务类标记，值范围从 0 到 7，每个值标识一个业务类型。

DSCP：DiffServ 的业务类标记，值的范围从 0 到 63，每个值标识一个业务类型。

内部 DSCP（internal DSCP）：交换机内部的 DSCP 值，交换机根据该值做 QoS 策略。

业务分类（classification）：在 QoS 域边界根据 IP 数据包的一个或多个字段对数据流进行分类，映射到一个内部 DSCP 值。

QoS 策略（Policing）：对业务类（内部 DSCP）采用的策略，包括是否做带宽处理，使用的优先级队列，是否修改 IP 数据包的业务类标记等。

QoS 信任端口（Trust Port）：只根据业务类标记进行 QoS 处理的交换机输入端口就是 QoS 信任端口，业务类标记可以是 COS，IP Precedence 和 DSCP，分别叫做 Trust COS，Trust IP_Precedence 和 Trust DSCP。在 QoS 域内的交换机的端口都是 QoS 信任端口。

QoS 非信任端口（Untrust Port）：直接对 IP 数据包做业务分类，在根据分类后得到的业务类进行 QoS 处理的交换机输入端口就是 QoS 非信任端口。在 QoS 域边界的交换机端口是 QoS 非信任端口。

In Profile：一个业务类的数据流在设定的带宽限制值内。

Out of Profile：一个业务类的数据流超过了设定的带宽限制值。

Mark：对 In Profile 和 Out of Profile 的业务类数据流的处理，对于 Out of Profile 的业务类数据流，丢弃，对于 In Profile 的业务类数据流，指定是否需要修改 IP 数据包的业务类标记以及修改的业务类标记的值是多少。

调度（scheduling）：根据调度策略对交换机输出端口各个优先级队列中的 IP 数据包进行优先级处理，把 IP 数据包发送出去。

FFP（Fast Filtering Processor）：快速过滤处理器，iSpirit 3626 交换机的硬件使用 FFP 实现业务分类和 QoS 策略。

- QoS 模型

如图 12-3 显示了 QoS 模型。在输入端口实现了 classification，policing，mark，介绍如下：

业务分类（classification）：对接收到 IP 数据包进行业务分类，生成一个内部 DSCP 值，为做 QoS 策略做准备。

QoS 策略（policing）：根据业务分类得到的内部 DSCP 值进行 QoS 处理，包括带宽限制，映射到一个优先级队列，产生业务类标记值。

Mark：对 Out of Profile 的数据流进行丢弃处理，对 In Profile 的数据流看是否需要修改数据流的业务类标记。

在输出端口实现了 Queuing 和 Scheduling，介绍如下：

存入队列（Queuing）：根据 QoS 策略得到的结果把 IP 数据包放入对应的输出优先级队列中进行缓存。

调度（Scheduling）：根据调度策略对存入队列中的 IP 数据包进行优先级处理并发送出去。

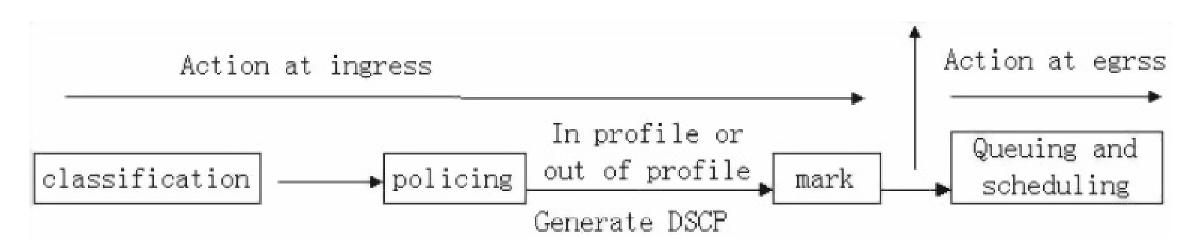


图 12-3　QoS 模型

● 业务分类

业务分类用于区分不同的数据流，根据数据流的一个或多个字段匹配进行分类，映射成一个内部 DSCP 值。只有启用 QoS 的交换机端口收到数据包才会进行业务分类，如果一个端口没有启用 QoS，则不进行业务分类，采用 best-effort 的方法进行转发。

对于 QoS 信任端口，业务分类比较简单，直接根据业务类标记进行分类，映射成内部 DSCP 值。如图 4 对业务分类的流程做了详尽的描述。

对于 Trust COS 端口，直接根据数据帧的 TAG 标记中的三位优先级进行分类，根据 COS-DSCP 映射表生成内部 DSCP 值，所有的数据流根据三位优先级最多可分成 8 类。注意：如果数据帧没有 TAG 标记，则认为其 COS 优先级值为 0，而不是端口缺省优先级（PPD-COS），数据帧如果从输出端口带标记发送出去，则其标记的 COS 优先级为输入端口的缺省优先级。

对于 Trust IP_Precedence 端口，直接根据 IP 数据包的 TOS 字段的最高三位进行分类，根据 PREC-DSCP 映射表生成内部 DSCP 值，所有的数据流根据三位 IP_Precedence 值最多可分成 8 类。

对于 Trust DSCP 端口，直接根据 IP 数据包的 TOS 字段的最高六位进行分类，根据 DSCP-DSCP 映射表生成内部 DSCP 值，所有的数据流根据六位 DSCP 值最多可分成 64 类。

对于 QoS 非信任端口，业务分类比较复杂，需要根据数据流的一个或多个字段进行分类，多个不同的数据流可以映射为一个业务类。iSpirit 3626 提供了 CLASS 和 POLICY 配置模式对数据流进行分类，在 CLASS 模式中，选择哪些数据流组成一个业务类，在 POLICY 模式中，把每个业务类映射为一个内部 DSCP 值，一个 POLICY 可以包括一个或多个 CLASS。如图 4 对业务分类的流程做了详尽的描述。

在 CLASS 模式中，可以有以下几种选择组成一个业务类：

选择一个或多个 COS（最多 8 个）组成一个业务类，称为 COS 业务类。

选择一个或多个 IP Precedence（最多 8 个）组成一个业务类，称为 PREC 业务类。

选择一个或多个 DSCP（最多 8 个）组成一个业务类，称为 DSCP 业务类。

选择一个（只能有一个）ACL 组组成一个业务类，称为 ACL 业务类。

对于基于 ACL 的业务分类，每个 ACL 组组成一个业务类，一个 ACL 组中有 1 条到 128 条规则，只有动作为 permit 的规则在 QoS 中才会生效，而动作为 deny 的规则在 QoS 中是无效的。ACL 组可以是标准 IP 组，扩展 IP 组，扩展 MAC 组。

在 POLICY 模式中，每个业务类可以映射成一个业务类标记值，业务类标记值再根据映射表生成一个内部 DSCP 值。如下：

业务类映射成 COS 业务类标记值，根据 COS-DSCP 映射表生成内部 DSCP 值。

业务类映射成 IP Precedence 业务类标记值，根据 PREC-DSCP 映射表生成内部 DSCP 值。

业务类映射成 DSCP 业务类标记值，根据 DSCP-DSCP 映射表生成内部 DSCP 值。

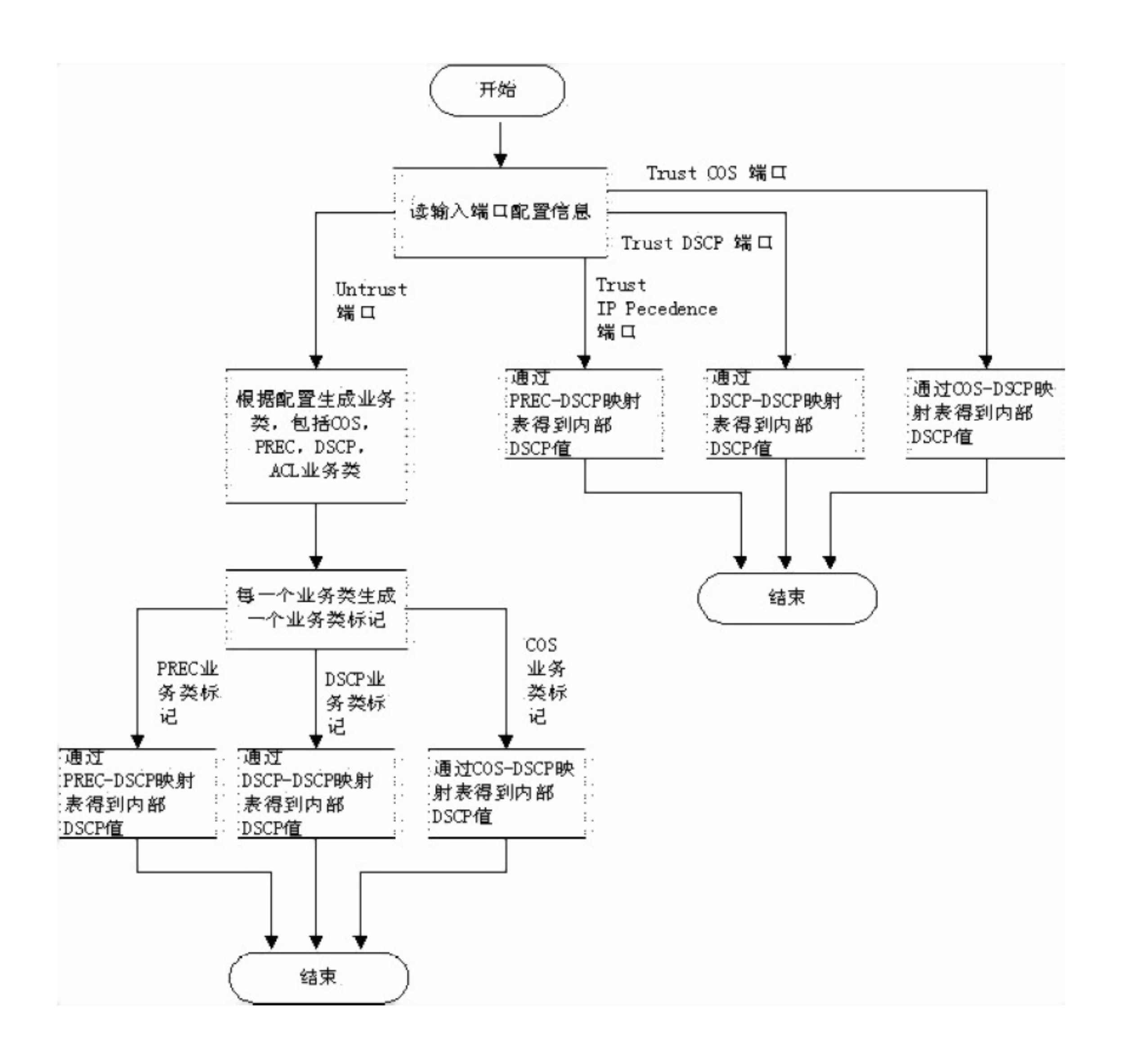


图 12-4　业务分类流程

● QoS 策略

QoS 策略包括 policing 和 mark 两个部分。当数据流分类后，需要采用一定的 QoS 策略对业务类进行 QoS 处理。QoS 策略主要包括以下内容：

决定业务类的带宽限制，是否在带宽限制内还是超过带宽限制。

决定业务类的优先级队列。

决定业务类标记，是否需要修改数据包，如何修改。

iSpirit 3626 交换机的每个输入端口都支持对每个数据流进行带宽限制，可以实现业务类的带宽限制处理，采用漏斗算法进行带宽限制处理，如图 5 所示。漏斗的深度 bucketsize 指的是能支持的最大突发数据流的大小，即 burstsize。当有匹配的数据流从输出端口流出时，相当与从漏斗流出，bucketcount 往下移动，当 bucketcount 处于 threshold 的

下方时，此时从输入端口流入的匹配数据流被限制住，处于 Out of Profile 状态。每隔 8us 系统根据设定的带宽限制值定时往漏斗中加 refreshcount 的流量，bucketcount 往上升，当处于 threshold 的上方时，数据流又允许流出，此时处于 In Profile 状态。当某个业务类处于 Out of Profile 状态时，丢弃后续输入的数据流，如果处于 In Profile 状态时，做进一步的处理。

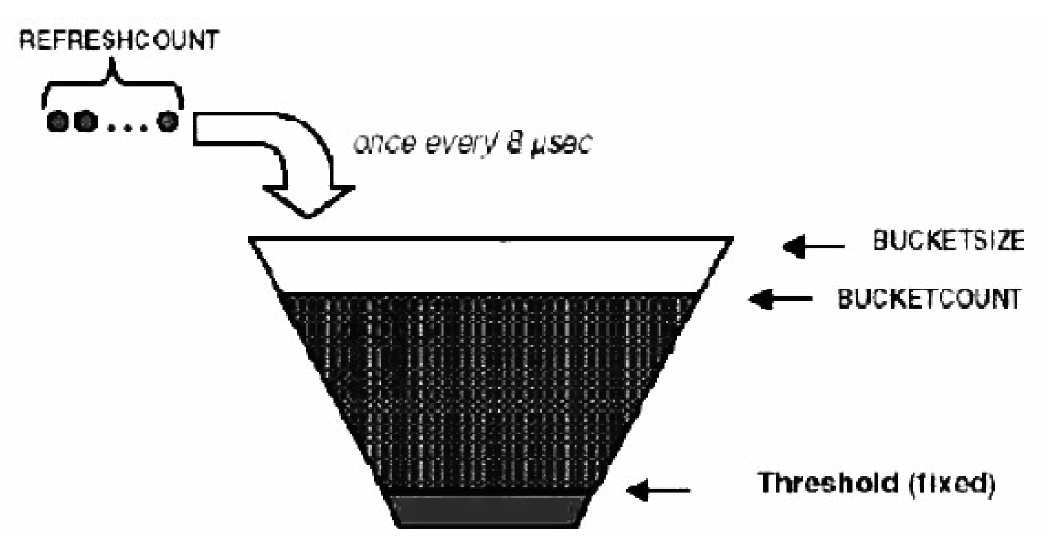


图 12-5　用于带宽限制的漏斗算法

当数据流处于 In Profile 状态时，可以做进一步处理，下一步要决定业务类送入输出端口的优先级队列。每一个业务类通过业务分类的步骤都得到一个内部 DSCP 值，通过 DSCP-QUEUE 映射表可以得到输出端口的优先级队列。iSpirit 3626 交换机的每个输出端口支持 4 个优先级队列。

业务类的业务类标记值在业务分类阶段已经得到，有三种业务类标记类型：COS 业务类标记，IP Precedence 业务类标记和 DSCP 业务类标记，在输出端口需要修改数据包对应字段，把业务类标记加在数据包中。

QoS 信任端口和非信任端口在 QoS 策略的处理上有很大的不同，QoS 信任端口只需要决定数据流的优先级队列，不需要做带宽限制和生成业务类标记值，也不修改 IP 数据包头。而 QoS 非信任端口则根据系统端口的配置情况进行 QoS 策略处理，确定业务类标记值，决定优先级队列是必须要做的，可以配置不做带宽限制处理。

● QoS 调度

iSpirit 3626 交换机的输出端口支持 4 个优先级队列，对列 1 优先级最低，队列 4 优先级最高。当数据流缓存在输出队列中后，输出端口需要根据配置的 QoS 调度方法对数据流做优先级处理，决定数据流的发送次序。iSpirit 3626 交换机的输出端口支持 3 种 QoS 调度方法，如下：

严格优先级调度（SPQ）：严格按照优先级对数据流进行调度，只有高优先级队列中的所有数据流发送出去后，才发送低优先级队列中的数据流。这种方法的缺点是低优先级队列中的数据流可能等待很长时间才得到处理。

循环调度（RR）：队列 1 到队列 4 的数据流按照相同的权重进行调度，实际上队列 1 到队列 4 的优先级是一样的。这种方法的缺点是不能保证重要数据的服务质量，实际上就跟没做 QoS 是一样的。

加权循环调度（WRR）：可以根据实际应用需要配置队列的权重，输出端口按照配置的队列权重对数据流进行调度。这种方法可以解决 SPQ 和 RR 调度方法的不足，可以保证重要数据的服务质量。

● FFP 简介

iSpirit 3626 交换机的每个端口的输入端有一个 FFP。FFP 可以实现业务分类和 QoS 策略。FFP 存在于硬件逻辑中，当端口启用 QoS 配置时，不会影响数据流的转发效率。

FFP 是一个共享资源，有多个应用会使用到 FFP，这些应用有：ACL 过滤，IP 地址绑定，QoS，IGMP SNOOPING 协议和 802.1x 协议等。FFP 中的条目有一定的限制，RULE 表中有 128 个条目，最多能对 128 个不同的数据流进行业务分类，如果 FFP 被其它应用占用，能支持的数据流个数会更少一些。FFP 中 METER 表中有 63 个条目，最多能对 63 个业务类（每个业务类可以包括多个数据流）做带宽限制。在实际使用中一定要注意合理使用 FFP 的资源。

如果系统启动了 IGMP SNOOPING 协议，系统中的每个端口的 RULE 表会占用一个条目。如果端口启用了 802.1x 协议，该端口的 RULE 表中会占用一个条目。如果端口启用了 ACL 过滤，根据 ACL 组中的规则个数占用 RULE 表中的条目。如果端口绑定了 IP 地址，根据 IP 地址绑定的个数为占用 RULE 表中的条目数。

12.2 QoS 配置

在做 QoS 配置之前，需要注意以下两点：

管理员先要了解网络中的实际应用以及交换机在 QoS 域中的位置，根据实际网络的需求做 QoS 配置。

iSpirit 3626 交换机根据每个端口启用 QoS，在启用 QoS 之前，要了解本端口的 FFP 的使用情况，本端口是否设置了 802.1x 和 ACL 过滤，本系统是否启用了 IGMP SNOOPING 协议等。

本节对 QoS 配置进行一个详细的描述，主要包括以下几部分内容：

- QoS 缺省配置
- 配置 QoS 映射表
- 配置 QoS 信任端口
- 配置 QoS 业务类
- 配置 QoS 策略
- 配置 QoS 非信任端口
- 配置 QoS 调度方法

● 1.QoS 缺省配置

iSpirit 3626 交换机缺省情况下所有的端口都没有启用 QoS，所有的数据流以 best-effort 的方法转发。

端口的缺省 COS 优先级为 0。

COS-DSCP 映射表缺省如图 6。

PREC-DSCP 映射表缺省如图 7。

DSCP-DSCP 映射表缺省如图 8。

DSCP-QUEUE 映射表缺省如图 9。

输出端口的 QoS 调度方法缺省为严格优先级调度（SPQ）。

COS值	0	1	2	3	4	5	6	7
内部DSCP值	0	8	16	24	32	40	48	56

图 12-6　COS-DSCP 映射表缺省值

IP Precedence值	0	1	2	3	4	5	6	7
内部DSCP值	0	8	16	24	32	40	48	56

图 12-7　PREC-DSCP 映射表缺省值

DSCP值	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
内部DSCP值	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
DSCP值	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
内部DSCP值	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
DSCP值	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
内部DSCP值	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
DSCP值	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
内部DSCP值	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63

图 12-8　DSCP-DSCP 映射表缺省值

内部DSCP值	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
队列QUEUEP值	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2

内部DSCP值	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
队列QUEUE值	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4

内部DSCP值	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
队列QUEUE值	5	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6

内部DSCP值	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
队列QUEUE值	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8

图 12-9　DSCP-QUEUE 映射表缺省值

- 2.配置 QoS 映射表

  所有的 QoS 映射表的配置和显示命令都在 CLI 全局 CONFIG 模式下输入。

- 下面的两条命令用于配置和显示 COS-DSCP 映射表：

  qos cos-dscp <cos-value> <internal-dscp-value>

  show qos cos-dscp

  例如把 COS 值 0 映射成内部 DSCP 值 40：

  Switch# qos cos-dscp 0 40

  Switch# show qos cos-dscp

- 下面的两条命令用于配置和显示 PREC-DSCP 映射表：

  qos prec-dscp <ip-precendence-value> <internal-dscp-value>

  show qos prec-dscp

  例如把 IP Precedence 值 0 映射成内部 DSCP 值 40：

  Switch# qos prec-dscp 0 40

  Switch# show qos prec-dscp

- 下面的两条命令用于配置和显示 DSCP-DSCP 映射表：

  qos dscp-dscp <dscp-value> <internal-dscp-value>

  show qos dscp-dscp

  例如把 DSCP 值 0 映射成内部 DSCP 值 40：

  Switch# qos dscp-dscp 0 40

  Switch# show qos dscp-dscp

- 下面的两条命令用于配置和显示 DSCP-QUEUE 映射表：

qos interdscp-queue <internal-dscp-value> <queue-id>

show qos interdscp-queue

例如把内部 DSCP 值 40 映射成队列 2：

Switch# qos interdscp-queue 40 2

Switch# show qos interdscp-queue

注意：

对映射表的配置只对后续端口启动的 QoS 有效，对于已经启动了 QoS 的端口，使用的是修改前的映射表。

● 3.配置 QoS 信任端口

QoS 信任端口包括 Trust COS 端口，Trust IP_Precedence 端口和 Trust DSCP 端口。QoS 信任端口的配置和显示命令在 PORT RANGE 配置模式下输入。

● 下面的命令用于配置 Trust COS 端口：

qos trust cos

例如端口 2，3 配置成 Trust COS 端口：

Switch(port 2-3)# qos trust cos

Switch(port 2-3)# show qos

● 下面的命令用于配置 Trust IP_Precedence 端口：

qos trust ip_precedence

例如端口 2，3 配置成 Trust IP_Precedence 端口：

Switch(port 2-3)# qos trust ip_precedence

Switch(port 2-3)# show qos

● 下面的命令用于配置 Trust DSCP 端口：

qos trust dscp

例如端口 2，3 配置成 Trust DSCP 端口：

Switch(port 2-3)# qos trust dscp

Switch(port 2-3)# show qos

● 下面的命令用于清除端口的 QoS 配置：

no qos

例如端口 2，3 清除端口的 QoS 配置：

Switch(port 2-3)# no qos

Switch(port 2-3)# show qos

注意：

如果配置 QoS 信任端口不成功，有三种可能性：该端口已经配置了 QoS（需要先清除端口的 QoS 配置，再对端口做 QoS 配置）、该端口的 FFP 被 ACL 过滤占用过多或该端口绑定了 IP 地址。Trust COS 需要占用 FFP 的 RULE 表中的 8 个条目，Trust IP_Precedence 需要占用 FFP 的 RULE 表中的 8 个条目，Trust DSCP 需要占用 FFP 的 RULE

表中的 64 个条目。

一个端口可以在配置为 QoS 信任端口的同时又做 ACL 过滤，可以先配置 ACL 过滤，再配置 QoS 信任端口，也可以先配置 QoS 信任端口，再配置 ACL 过滤。

● 4.配置 QoS 业务类

QoS 业务类包括四种：COS 业务类、PREC 业务类、DSCP 业务类和 ACL 业务类。

在选择一个业务之前需要创建一个 QoS 类，在全局 CONFIG 模式下输入下面的命令创建一个 QoS 类，并进入 CLASS 配置模式。class-id 的范围从 1 到 1000。

qos class <class-id>

在 CLASS 模式下，可以给 QoS 类取一个名字用于标识该类：

name <class-name>

例如创建一个 QoS 类，class-id 为 3，名字为 abc：

Switch# qos class 3

Switch(class-3)# name abc

Switch(class-3)# show qos class 3

在 CLASS 配置模式下，给 QoS 类选择一种业务流。

● 下面的命令给 QoS 类选择 COS 业务流，形成 COS 业务类，最多可以输入 8 个 COS 值，如果输入的值相同，相同的值认为是一个：

match cos <cos-value> [cos-value] …

● 下面的命令给 QoS 类选择 IP Precedence 业务流，形成 PREC 业务类，最多可以输入 8 个 IP Precednece 值，如果输入的值相同，相同的值认为是一个：

match ip_precedence <ip-precedence-value> [ip-precedence-value] …

● 下面的命令给 QoS 类选择 DSCP 业务流，形成 DSCP 业务类，最多可以输入 8 个 DSCP 值，如果输入的值相同，相同的值认为是一个：

match dscp <dscp-value> [dscp-value] …

● 下面的命令给 QoS 类选择 ACL 业务流，形成 ACL 业务类，一个 QoS 类只能选择一个 ACL 组，选择的 ACL 组必须存在：

match acl <acl-id>

例如一个 QoS 类 3 选择 DSCP 值 20、40，45、60 作为一个 DSCP 业务类：

Switch(class-3)# match dscp 20 40 45 60

Switch(class-3)# show qos class 3

在全局 CONFIG 模式下输入下面的命令删除一个 QoS 业务类：

no qos class <class-id>

例如删除业务类 3：

Switch# no qos class 3

Switch# show qos class 3

注意：

一个 QoS 类只能是 COS 业务类、PREC 业务类、DSCP 业务类和 ACL 业务类中的一种。

一个 QoS 业务类可以被多个 Policy 引用。

当一个 QoS 业务类被一个或多个 Policy 引用时，这个 QoS 业务类不能被删除和修改。

● 5.配置 QoS 策略

iSpirit 3626 交换机总共支持 26 个 QoS 策略，每一个 QoS 策略可以选择一个或多个 QoS 业务类，对每一个 QoS 业务类配置对应的策略。

在全局 CONFIG 模式下输入下面的命令选择一个 QoS 策略，进入 POLICY 模式，policy-id 的范围从 1 到 26：

qos policy <policy-id>

在 POLICY 配置模式下输入下面的命令选择一个业务类，进入 POLICY CLASS 模式，选择的业务类必须存在并且状态必须为 active：

class <class-id>

在 POLICY CLASS 模式下，对选择的业务类配置策略，包括配置业务类标记和配置带宽限制。

业务类标记包括三种：COS 业务类标记、IP Precedence 业务类标记和 DSCP 业务类标记。

● 下面的命令对业务类配置 COS 业务类标记：

set cos <cos-value>

● 下面的命令对业务类配置 IP Precedence 业务类标记：

set ip_precedence <ip-precedence-value>

● 下面的命令对业务类配置 DSCP 业务类标记：

set dscp <dscp-value>

一个业务类在做 QoS 策略配置时，可以配置带宽限制策略，也可以不配置。如果配置带宽限制时，最小带宽限制值为 1Mbps，粒度为 1Mbps。下面的命令在 POLICY CLASS 模式下配置业务类的带宽限制：

meter <bandwidth-value> <burst-size>

● 下面的命令用于取消业务类的带宽限制，即业务类不做带宽限制策略：

no meter

在全局 CONFIG 模式下输入下面的命令清除 QoS 策略中的一个或所有的业务类，如果不输入 class-id，则清除 QoS 策略中的所有的业务类，如果输入 class-id，则清除指定的业务类：

no qos policy <policy-id> [class-id]

● 下面举一个 QoS 策略配置的示例：

Policy 2 中包括两个业务类：Class 3 和 Class 4。Class 3 和 Class 4 都是 ACL 业务类，分别匹配 IP 标准 ACL 组 3 和 IP 扩展 ACL 组 203。Class 3 配置 DSCP 业务类标记，值为 40，限制带宽到 2Mbps，Class 4 配置 IP Precedence 业务类标记，值为 6，不限制带宽。配置如下：

Switch# qos class 3　　（创建业务类 3）

Switch(class-3)# match acl 3　　（业务类 3 为 ACL 业务类，选择 ACL 组 3，假设 ACL 组 3 已经存在）

Switch(class-3)# qos class 4　　（创建业务类 4）

Switch(class-4)# match acl 203　　（业务类 4 为 ACL 业务类，选择 ACL 组 203，假设 ACL 组 203 已经存在）

Switch(class-4)# exit　　（退出 CLASS 配置模式）

Switch# show qos class （显示业务类配置情况）

Switch# qos policy 2 （进入 POLICY 配置模式）

Switch(policy-2)# class 3 （选择业务类 3，进入 POLICY CLASS 模式，可以对业务类 3 进行 QoS 策略配置）

Switch(policy-map-class 3)# set dscp 40 （设置 DSCP 业务类标记值）

Switch(policy-map-class 3)# meter 2 0 （设置业务类 3 的带宽限制）

Switch(policy-map-class 3)# exit （退出 POLICY CLASS 模式）

Switch(policy-2)# class 4 （选择业务类 4，进入 POLICY CLASS 模式，可以对业务类 4 进行 QoS 策略配置）

Switch(policy-map-class 4)# set ip_precedence 6 （设置 IP Precedence 业务类标记值）

Switch(policy-map-class 4)# show qos policy 2 （显示 Policy 2 的配置）

注意：

一个 QoS 策略可以选择一个或多个 QoS 业务类，最多可以选择 128 个业务类。

一个 QoS 策略中的一个业务类只能配置 COS 业务类标记值、IP Precedence 业务类标记值和 DSCP 业务类标记值中的一种。

一个 QoS 策略可以被一个或多个非信任端口引用。

当一个 QoS 策略被一个或多个非信任端口引用时，该 QoS 策略不能被删除和修改。

● 3.配置 QoS 非信任端口

配置 QoS 非信任端口实际上就是端口选择一个 QoS 策略。下面的命令用于在 PORT RANGE 模式下配置非信任端口，选择的 policy-id 必须存在并且状态必须为 active。

qos service-policy <policy-id>

例如端口 2，3 选择 Policy 2 配置非信任端口：

Switch(port 2-3)# qos service-policy 2

Switch(port 2-3)# show qos

如果非信任端口配置不成功，可能有以下几种情况：

该端口已经配置成 QoS 信任端口或 QoS 非信任端口。

选择的 QoS 策略不存在或其状态不为 active。

该端口已经绑定了一个或多个 IP 地址。

该端口的 FFP 的 RULE 表空间不足，可能是：该端口已经做了 ACL 过滤或 QoS 分类的数据流过多。每个端口的 FFP 的 RULE 表的空间有 128 个条目。

该端口的 FFP 的 METER 表空间不足，可能是 QoS 策略中做带宽限制的业务类太多，超过了 63 个，这种情况比较少出现。FFP 的 METER 表的空间有 63 个条目。

QoS 策略中的两个或多个 ACL 业务类，每个 ACL 业务类匹配一个 ACL 组，这些组中有相同的两条过滤规则。

对于第 6 点，举例如下：

ACL 组 2 配置 2 条规则：

Switch# access-list 2 permit 192.168.0.0 0.0.0.255

Swtich# access-list 2 permit 192.168.1.0 0.0.0.255

ACL 组 3 配置 1 条规则，该条规则与 ACL 组 2 中的 1 条规则相同

Switch# access-list 3 permit 192.168.0.0 0.0.0.255

QoS 类 2 配置为 ACL 业务类，ACL 组为 2：

Switch# qos class 2

Switch(class-2)# match acl 2

QoS 类 3 配置为 ACL 业务类，ACL 组为 3：

Switch(class-2)# qos class 3

Switch(class-3)# match acl 3

配置 QoS 策略 2，选择业务类 2 和业务类 3：

Switch(class-3)# qos policy 2

Switch(policy-2)# class 2

Switch(policy-map-class 2)# set dscp 30

Switch(policy-map-class 2)# exit

Switch(policy-2)# class 3

Switch(policy-map-class 3)# set dscp 40

设置端口 2 为非信任端口，选择 Policy 2：

Switch(port 2)# qos service-policy 2

此时 QoS 非信任端口不能配置成功，因为 ACL 组 2 和组 3 有相同的 ACL 规则。

- 下面的命令在 PORT RANGE 模式下清除端口的 QoS 配置：

  no qos

- 如端口 2，3 原来配置为非信任端口，选择了 Policy 2 作为其策略，现在清除端口的 QoS 配置：

  Switch(port 2-3)# no qos

  Switch(port 2-3)# show qos

  注意：

每个端口只能配置为 Trust COS, Trust IP_Precedence、Trust DSCP 和非信任端口中的一种，如果配置为非信任端口，只能选择一个 QoS 策略。

一个端口可以配置 QoS 非信任端口的同时做 ACL 过滤，但必须先配置 ACL 过滤，再配置 QoS 非信任端口，如果已经配置了 QoS 非信任端口，此时配置 ACL 过滤会失败，必须先删除此端口的 QoS 配置再设置 ACL 过滤。

一个端口配置为 QoS 非信任端口时，QoS 策略中的 ACL 业务类的“permit”动作的 ACL 规则会写入 FFP，“deny”动作的 ACL 规则不会写入 FFP，也就是说“deny”动作的 ACL 规则不会对数据流做 QoS。

如果一个 QoS 策略中的两个或多个的业务类有相同的匹配值，则第一个配置的业务类中的匹配值做 QoS，后面配置的相同的匹配值不会做 QoS。如一个 COS 业务类有一个匹配的 COS 值 5，另一个 COS 业务类也有一个匹配的 COS 值 5，则第一个配置的 COS 值为 5 的做 QoS。建议用户在配置时不要配置重复的匹配值。

- 7.配置 QoS 调度方法

iSpirit 3626 对所有端口的输出端做同样的 QoS 调度，iSpirit 3626 交换机支持 3 种调度方法：严格优先级调度（SPQ），循环调度（RR），加权循环调度（WRR）。对于 WRR，每个优先级队列必须有一个权重，队列 1 到 4 的缺

省权重分别为 1、2、3、4，可以对优先级队列的权重进行配置，权重的范围是 1 到 15。

在 PORT RANGE 模式下配置端口的 QoS 调度方法。

- 下面的命令配置端口的 QoS 的调度方法为 SPQ：

  qos schedule spq

- 下面的命令配置端口的 QoS 的调度方法为 RR：

  qos schedule rr

- 下面的命令配置端口的 QoS 的调度方法为 WRR，可以不输入权重，如果输入权重，必须输入队列 1 到 4 的权重：

  qos schedule wrr [<queue1-weight> <queue2-weight>…<queue4-weight>]

  例如配置端口为 WRR 调度方法，队列 1 到 4 的权重分别为 1、3、5、7：

  Switch# qos schedule wrr 1 3 5 7

  Switch# show schedule

第 13 章 配置 IP 路由

本章描述如何在 iSpirit 3626 交换机上配置 IP 路由，包含内容如下：

1、IP 路由介绍

2、接口配置

3、ARP 配置

4、静态路由配置

5、相关配置示例

13.1 IP 路由介绍

路由功能是三层交换机的重要功能之一，能够实现在不同 IP 网段间的高速路由转发。

iSpirit 3626 是一款三层交换机，具备三层转发功能；但是它可以通过其它的三层设备访问不同网段的设备。

有三种方式实现路由

- 缺省路由：当数据流目的地址未知时，把数据流导向某特定出口。
- 静态路由：由用户指定配置的路由，使数据流从指定端口沿单一路径输出到某网络。
- 动态路由：通过动态路由协议计算最佳路径并转发数据流。

1.接口配置

配置 IP 路由，必须为三层接口分配 IP 地址，之后三层接口内的主机才能同其他三层接口内的主机通讯。某些特殊的地址是不能分配给三层接口的，详见下表。

表 13-1：

类	地址或地址范围	是否可分配
A	0.0.0.0	否
	1.0.0.0 – 126.0.0.0	是
	127.0.0.0	否
B	128.0.0.0 – 191.254.0.0	是
	191.255.0.0	否
C	192.0.0.0	否
	192.0.1.0 – 223.255.254.0	是
	223.255.255.0	否
D	224.0.0.0 – 239.255.255.255	多播组地址
E	240.0.0.0 – 255.255.255.254	否
	255.255.255.255	广播地址

2.命令

- 进入某个 interface vlan 配置模式：

  Switch# interface vlan <vlan id>
- 为某个 interface vlan 配置 ip 子网，即设置接口 ip 地址：

  Switch(interface-vlan)# ip address <ipaddress> <subnetmask>
- 删除某个 interface vlan 对应的 ip 子网：

  Switch# no interface vlan <vlan id>
- 显示交换机子网接口信息：

  Switch(route-config)#show ip subnet
- 显示交换机某个或多个 vlan interface 信息：

  Switch# show interface vlan [<vlan_id>|<vlan_id_min-vlan_id_max>]

3.实例

- 为 interface vlan 3 配置子网 193.1.1.0，接口 ip 地址为 193.1.1.1：

  Switch(interface-vlan 3)# ip address 193.1.1.1 255.255.255.0
- 现在欲删除该 interface vlan 的子网：

  Switch# no interface vlan 3 或 Switch(interface-vlan 3)# no interface vlan 3

13.2 ARP 配置

1.ARP概述

ARP（Address Resolution Protocol）是为 IP 地址到对应的硬件地址提供映射的协议。当源端把以太网数据帧发送到位于同一局域网的目的端时，是根据 48 位的以太网地址来确定目的接口的。设备驱动程序从不检查 IP 数据报中的目的 IP 地址。所以需要通过 ARP 协议来得到 IP 地址相应的以太网地址。

2.ARP高速缓存

每台设备上都有一个 ARP 高速缓存，这个高速缓存存放了最近 IP 地址到硬件地址之间的映射记录。高速缓存中每一项都有其生存时间，当某表项长期未被使用，将被删除。

3.ARP表项分类

静态 ARP：用户手动配置的 ARP 表项，系统不会自动刷新或删除。

动态 ARP：系统自动完成的 IP 地址和以太网地址对应关系的探测，并能够实时更新和维护。

4.ARP命令

- 设置静态 ARP 项：

  Switch# arp <ip> <mac>
- 删除静态 ARP 项：

  Switch# no arp <ip>
- 显示系统 ARP 表内容：

  Switch# show arp

实例

设置目的 ip 为 200.1.1.2 ，mac 地址为 00:10:5f:01:02:03 的静态 ARP 项：

Switch# arp 200.1.1.2 00:10:5f:01:02:03

把这个静态 ARP 项删除：

Switch# no arp 200.1.1.2

13.3 配置静态路由

1.概述

用户在路由模式下配置交换机的静态路由信息。静态路由是由用户定义的、一条可使数据包从源地址通过指定路径到达目的地址的路由。当动态路由协议未能创建一条到特定目的的路由时，静态路由就显得特别重要。还可以通过配置某一静态路由为缺省路由，把无法确定路由的数据包发送到默认的网关。

静态路由是由管理员手工配置而成。适用于组网结构较简单、到给定目标只有一条路径的网络中，管理员只需配置静态路由就能使交换机正常工作。静态路由于不会有路由更新而不会占用宝贵的网络带宽。

缺省路由也是一种静态路由。简单地说，缺省路由就是在没有找到任何匹配的路由项情况下，才使用的路由。即只有当无任何合适的路由时，缺省路由才被使用。在路由表中，缺省路由以到网络 0.0.0.0（掩码为 0.0.0.0）的路由形式出现。可通过命令 show ip route table 来查看它是否被设置。若报文的目的地不在路由表中且路由表中也无缺省路由存在，该报文被丢弃的同时将返回源端一个 ICMP 报文指出该目的地址或网络不可达信息。缺省路由在网络中是非常有用的。在一个包含上百个交换机的典型网络中，运行动态路由选择协议可能会耗费较大量的带宽资源，使用缺省路由就可节约因路由选择所占用的时间与包转发所占用的带宽资源，这样就能在一定程度上满足大量用户同时进行通信的需求。

2.命令

- 设置静态路由

  Switch(route-config)# ip route <dst> <subnet> <nexthop>

- 删除静态路由

  Switch(route-config)# no ip route <dst> <subnet>

- 显示静态路由表内容：

  Switch(route-config)# show ip static route

- 显示所有的路由表内容（包括动态路由和静态路由）：

  Switch(route-config)# show ip route

3.实例

- 设置目的地址 ip 为 200.1.1.0，子网掩码为 255.255.255.0，下一跳为 10.1.1.2 的静态路由：

  Switch(route-config)# ip route 200.1.1.0 255.255.255.0 10.1.1.2

- 删除目的地址 ip 为 200.1.1.0，子网掩码为 255.255.255.0，下一跳为 10.1.1.2 的静态路由：

  Switch(route-config)# no ip route 200.1.1.0 255.255.255.0

第 14 章 配置 RIP

本章对 RIP 协议及其配置进行详细的介绍，主要包括以下内容：

1、RIP 介绍

2、RIP 配置

3、RIP 配置示例

14.1 RIP 介绍

RIP 是 Routing Information Protocol （即路由信息协议）的简称,是 Internet 中常用的路由协议。它是一种内部路由协议。RIP 采用距离向量算法，即路由器根据距离选择路由，所以也称为距离向量协议。RIP 是一种基于 V-D 算法的协议，它通过 UDP（User Datagram Protocol）数据报交换路由信息，每隔 30 秒向外发送一次路由更新。如果路由器经过 180 秒没有收到来自对端的路由更新信息，则将所有来自此路由器的路由信息标志为不可达，并且如果在其后 120 秒内仍没有收到更新信息就将其删除。RIP 运行简单，适用于小型网络.

RIP 使用跳数（hop count）来衡量到达信宿机的距离，称为路由权（Routing Metric）。在 RIP 中路由器到与它直接相连的网络的跳数为 0（在某些协议中被定义为 1），到通过一个路由器可达的网络的距离为 1 跳，其余依此类推。为限制收敛时间，RIP 规定 metric 为 1~15 间的整数，若跳数超过或等于 16 位被当作无穷大。

RIP 有 RIP-1 和 RIP-2 两个版本，RIP-2 支持明文认证和 MD5 密文认证，并支持可变长子网掩码。

RIP 启动和运行的整个过程可描述如下：

(1) 某路由器刚启动 RIP 时，以广播形式向其相邻路由器发送请求报文，相邻路由器收到请求报文后，响应该请求，并回送包含本地路由信息的响应。

(2) 路由器收到响应报文后，修改本地路由表，同时向相邻路由器发送触发修改报文，广播路由修改信息。相邻路由器收到触发修改报文后，又向其各自的相邻路由器发送触发修改报文。在一连串的触发修改广播后，各路由器都能得到并保持最新的路由信息。

(3) 同时，RIP 每隔 30 秒向其相邻路由器广播本地路由表，相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络广播修改信息，使更新的路由最终能达到全局有效。同时，RIP 采用超时机制对过时的路由进行超时处理，以保证路由的实时性和有效性。RIP 作为 IGP 协议的一种，正是通过这些机制，使路由器能够了解到整个网络的路由信息。

例：下图所示为 RIP 协议的运行过程。

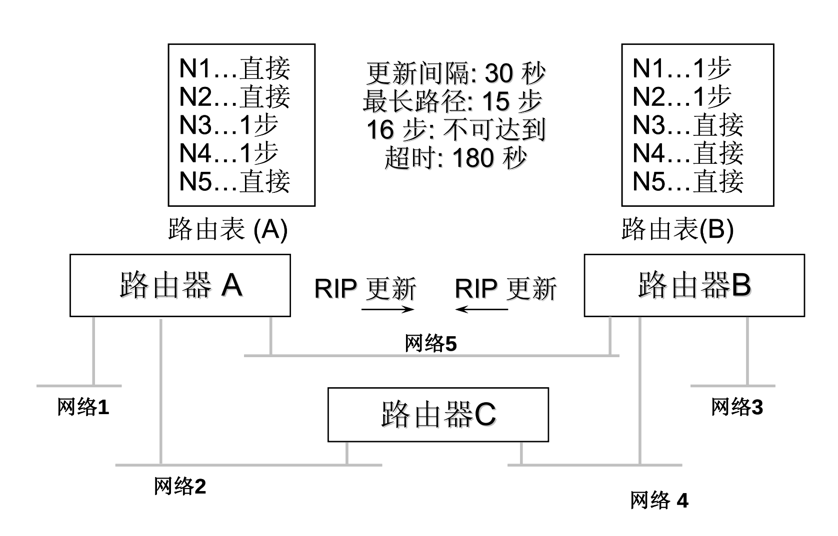


图 14-1　RIP 协议工作过程

在网络 5: 路由器 A 每隔 30 秒钟向自己的邻居广播自己的路由表.

在网络 5: 路由器 B 每隔 30 秒钟向自己的邻居广播自己的路由表.

路由器 A 和 B 更新自己的路由表.

路由器不能有超过 15 的步长值. 如果步长为 16 则认为网络是不可到达的.

如果路由器有 6 次(缺省 = 180 秒) 不能收到期望的路由器更新，则当它自己广播时,就会宣布前面收到的路由是非法的.

虽然 RIP 目前已被大多数路由器厂商所广泛使用，但它还是有较大的局限性：

支持站点的数量有限：这就使得 RIP 只适用于较小的自治系统，如只用于大多数校园网及结构较简单的连续性强的地区性网络。

依靠固定度量计算路由：RIP 不能实时更新度量值来适应网络发生的变化，在人为更新之前，由网络管理员定义的度量值仍是固定不变的。

路由表更新信息将占用较大的网络带宽：RIP 每 30 秒就向外广播发送路由更新信息。在有许多节点的网络中，这样将消耗相当大的网络带宽。

14.2 RIP 配置

包含 rip 路由的基本配置的设置、静态路由的重分发、以及察看等相关的指令：

启动 RIP 协议, 参数为协议名称 rip

Switch# ip protocol rip

关闭 RIP 协议, 参数为协议名称 rip

Switch# no ip protocol rip

进入 RIP 配置模式

Switch# rip

按接口打开 RIP 协议，要求输入接口

Switch(rip_config)# rip on <interface-address>

按接口关闭 RIP 协议，要求输入接口

Switch(rip_config)# rip off <interface-address>

显示 rip 协议配置信息，带参数是显示指定接口的配置信息，不带参数是显示所有接口的配置信息

Switch(rip_config)# show rip [ipaddr]

显示整个 RIP 路由表

Switch(rip_config)# show table

配置 rip 协议的认证 type，这是一个交互式命令，首先要求输入接口 ipaddr，

然后是 authentication type，可以是"text"，"md5"两种形式, "no"表示无认证。

Switch(rip_config)# auth type <interface-address> <type-word>

配置 rip 协议的认证密码，这是一个交互式命令，首先要求输入接口 ipaddr，

然后是 authentication key。当使用 md5 方式时，要求认证双方的 key id 与 key 均相同。key id 为 key 输入的顺序，当前认证所采用的 key 为最后输入的 key， 所以认证双方须输入相同个数的 key。Key 的有效期为一年。当不采用 md5 认证方式时（auth type 命令，输入 no），原来配置的所有 key 将被删除。

Switch(rip_config)# auth key <interface-address> <key-word>

配置 rip 协议的 send type,首先要求输入接口 ipaddr；然后是 send type，可以为"nosend ", "v1 ", "v2 ", "v1 compatible ","v1demand ", "v2demand "

Switch(rip_config)# send type <interface-address> <type-word>

配置 rip 协议的 receive type，首先要求输入接口 ipaddr；然后是 rece ive ty pe,可以为"v1 "， "v2 "， "v1|v2"，"noreceive"。

Switch(rip_config)# receive type <interface-address> <type-word>

配置 rip 协议的默认跳数, 这是一个交互式命令，首先要求输入接口

ipaddr， 然后是 default met ric，距离大小是 1-15

Switch(rip_config)# default metric

将静态路由信息重新分发到 rip 协议

Switch(rip_config)# redistribute

示例:

Switch(rip_config)# red

Protocol Name(static):static

Default Metric(0-15):2

static is transferred now

关闭 redistribution 功能，用户可选择是否保存原有路由

Switch(rip_config)# no redistribute

示例:

Switch(rip_config)# no red

Protocol Name(static):static

Keep old routes(Yes/No):yes

显示所有接口的 redistribution 信息

Switch(rip_config)# show redistribute

显示端口收发各种报文的统计信息

Switch(rip_config)# show stats

14.3 RIP 配置示例

实例一

1．配置环境：

三台交换机两两相连，分别有 6 个网段，都启用 rip 协议，实现三台 PC 机之间能够两两互通。

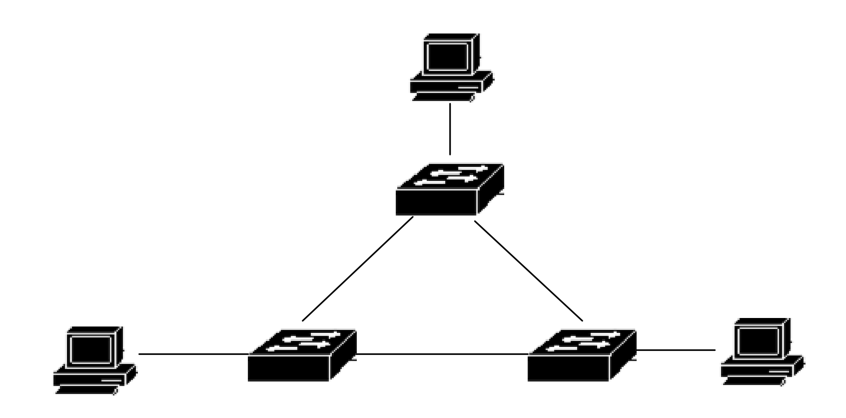


图 14-2 组网示例一

2．配置步骤：

(1) 在每台交换上配置

Switch# ip protocol rip

(2) 启用 rip 协议（默认情况下 rip 协议是关闭的）

(3) 配置三层交换机 A 的 RIP 路由协议：

Switch# RIP

Switch(rip_config)# rip on 1.1.1.2

Switch(rip_config)# rip on 1.1.2.1

Switch(rip_config)# rip on 1.1.6.1

(4) 配置完成以后用 show rip 进行查看

Switch(rip_config)# show rip

```
————————————————————————————————
| Ip Address | Auth Type | Auth Key | Send Type | Recv Type| Mc | State |
|————— +—————— +———— +—————— +———— +—— +——— |
| 1.1.1.2 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |
| 1.1.2.1 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |
| 1.1.6.1 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |
|————— +—————— +———— +—————— +———— +—— +——— |
————————————————————————————————
```

(5) 配置三层交换机 B 的 RIP 路由协议：

Switch# RIP

Switch(rip_config)# rip on 1.1.3.2

Switch(rip_config)# rip on 1.1.4.1

Switch(rip_config)# rip on 1.1.6.2

(6) 配置完成以后用 show rip 进行查看

Switch(rip_config)# show rip

```
———————————————————————
| Ip Address | Auth Type | Auth Key | Send Type | Recv Type| Mc | State |
|———— +——— +——— +——— +——— +—— +— |
| 1.1.3.2 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |
| 1.1.4.1 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |
| 1.1.6.2 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |
|——— +——— +———— +——— +— +—— +——— ———————————————
—————————
```

(7) 配置三层交换机 C 的 RIP 路由协议：

Switch# RIP

Switch(rip_config)# rip on 1.1.2.2

Switch(rip_config)# rip on 1.1.3.1

Switch(rip_config)# rip on 1.1.5.2

(8) 配置完成以后用 show rip 进行查看

Switch(rip_config)# show rip

——————————————————————————————————————

| Ip Address | Auth Type | Auth Key | Send Type | Recv Type| Mc | State |

|—————— +—————— +———— +—————— +———— +—— +——— |

| 1.1.2.2 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |

| 1.1.3.1 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |

| 1.1.5.2 | no Auth | |rip1Compatbl|rip1Orip2| 0 | Active |

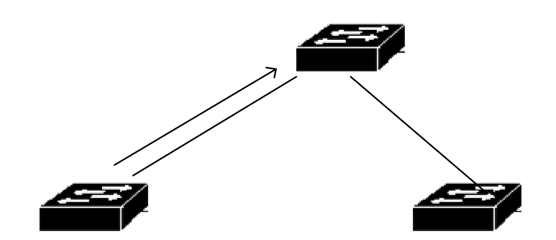
|—————— +—————— +———— +—————— +———— +—— +——— |

—————————————————————————————————————

实例二

1．配置环境：

三层交换机 A 与 B， A 与 C 分别相连，若交换机 A（192.1.1.1）只想把路由更新信息发送到相邻交换机 B（ 192.1.1.2）而不发给相邻交换机 C。



2.配置步骤

(1) 进入交换机 A 的路由模式

(2) 设置交换机 A 某一接口的发送类型为“nosend”

Switch(rip_config)# send type 192.1.1.1 nosend

第 15 章 配置 IGMP

在传统的 Internet 中,采用单播的方式将数据包发送给网络中的各个接收者,随着网络中的使用节点的增多,发出包的数量也会线性的增加。如果传输数据相同（例如，网络视频会议，电视直播等，对于不同的节点同一时间接收到的数据实际上是相同的），这将使得发送主机、路由设备及带宽资源总体负担加重，效率严重增加。随着网络视频会议，视频直播应用等需求的增长，为了提高资源的利用率，组播方式日益成为多点通信中普遍采用的传输方式。

在需要向多个主机发送多媒体信息（如音频、视频直播）的情况下，分别向每一客户端主机发送数据并不是个非常有效的方法，如果采用广播的方法，又存在发送主机与某些接收端的客户主机不在同一子网的情况，因而采用广播方式也不是一个好的解决方案。下图对单播和组播两种方式进行了比较。

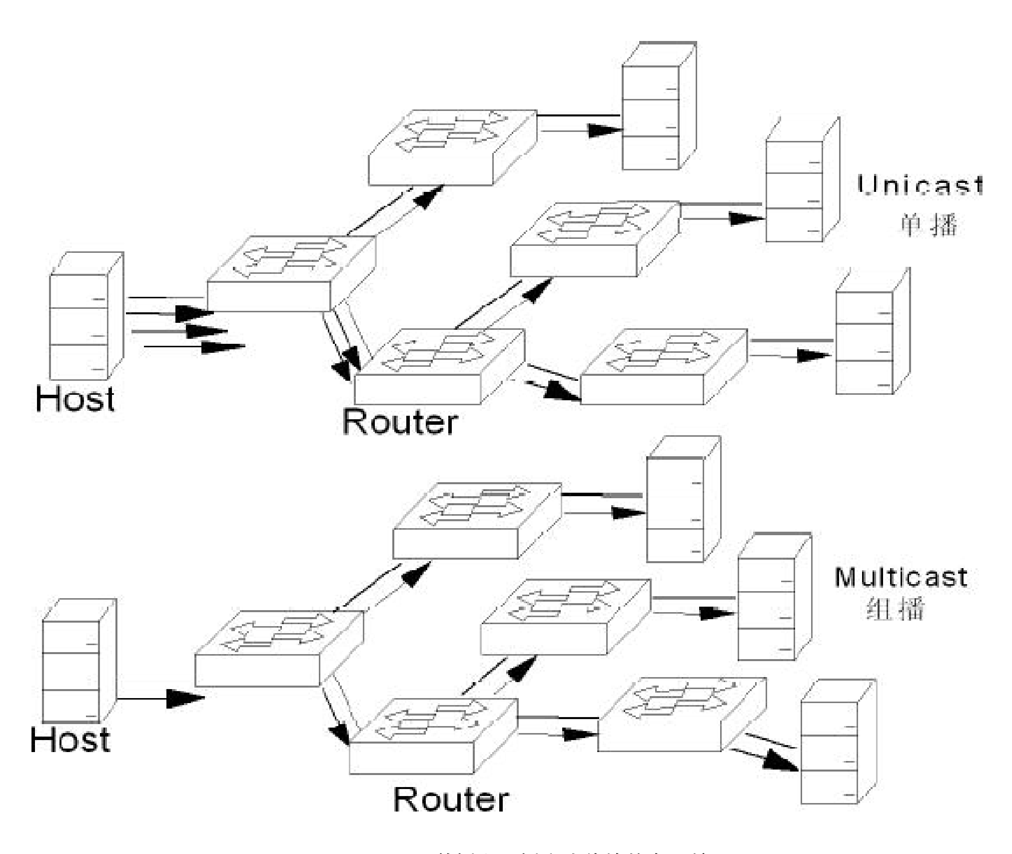


图 15-1　单播和组播方式传输信息比较

从图 14-1 中可以看出为了传递数据给三个终端，采用单播方式，需要发送三个内容相同的数据包，而采用组播方式则只需要一个到组播组的数据包即可，在复杂环境中，如此可以显著提高资源利用率。

组播技术主要由 IGMP 协议和组播路由协议来支持实现,其中 IGMP 协议主要控制用户加入和离开组播组的管理，而组播路由协议则是来构造路由器间的组播路径。

IGMP 协议主要实现组播用户组的管理，主机通过 IGMP 协议告诉路由器希望加入或者离开某一个组，组播路由器通过 IGMP 协议可以判断在它所直接相连的子网中是否存在组播组成员。

本章对 IGMP 相关的基本概念、IGMP 协议实现和 IGMP 配置进行详细的描述，主要包括以下部分内容：

1、IGMP 相关的基本概念

2、IGMP 协议实现

3、IGMP 配置

15.1 IGMP 相关的基本概念

本节对 IGMP 相关的基本概念进行描述，主要包括以下内容：

- 组播地址
- 组播 MAC 地址
- 两个特殊的组播地址
- IGMPV2 的消息格式

1.组播地址

在网络中，主机间以如下三种不同的地址进行通信：

- 单播地址：子网中主机的唯一地址。如 IP 地址：10.10.1.9 或 MAC 地址：01:00:5C:A0:4A:B1。
- 广播地址：这种类型的地址用来向子网内的所有主机发送数据。如广播 IP 地址是 192.168.100.255，MAC 广播地址：FF:FF:FF:FF:FF。
- 组播地址：通过该地址向多个主机即主机群发送数据。

IP 地址空间被划分为 A、B、C 三类。第四类即 D 类地址被保留用做组播地址。在第四版的 IP 协议（IPv4）中，从 224.0.0.0 到 239.255.255.255 间的所有 IP 地址都属于 D 类地址。

组播地址为高四位为“1110”的地址，对应到十进制是 224 到 239，其它 28 位保留用做组播的组标识，如图 2 所示：

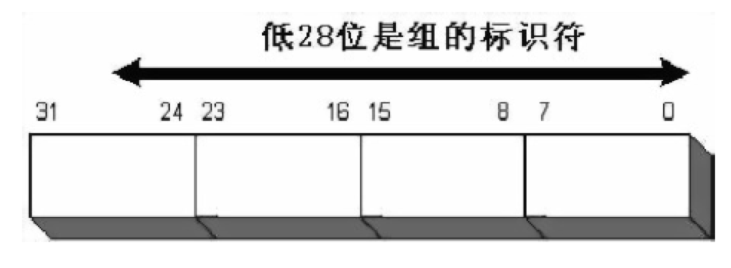


图 15-2　组播地址

2.组播MAC地址

IPv4 的组播地址在网络层要转换成网络物理地址（MAC 地址）。对一个单播的网络地址，通过 ARP 协议可以获取与 IP 地址对应的物理地址。但在组播方式下 ARP 协议无法完成类似功能，必须得用其它的方法获取物理地址。以下 RFC 文档中提出了完成这个转换过程的方法：

- RFC1112：Multicast IPv4 to Ethernet physical address correspondence
- RFC1390：Correspondence to FDDI
- RFC1469：Correspondence to Token-Ring networks

在最大的以太网地址范围内，转换过程是这样的：将以太网物理地址（MAC 地址）的前 24 位固定为 01:00:5E，

这几位是重要的标志位。紧接着的一位固定为 0，其它 23 位用 IPv4 组播地址中的低 23 位来填充。该转换过程如图 3 所示：

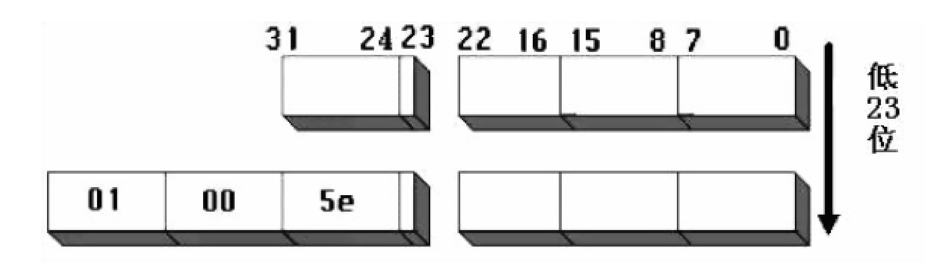


图 15-3　组播 IP 地址到组播 MAC 地址的转换

例如，组播地址为 224.0.0.5 其以太网物理地址（MAC 地址）为 01:00:5E:00:00:05。

3.两个特殊的组播地址

224.0.0.1：标识子网中的所有主机。同一个子网中具有组播功能的主机都是这个组的成员。

224.0.0.2：该地址用来标识网络中每个具有组播功有的路由器。

4. IGMPV2的消息格式

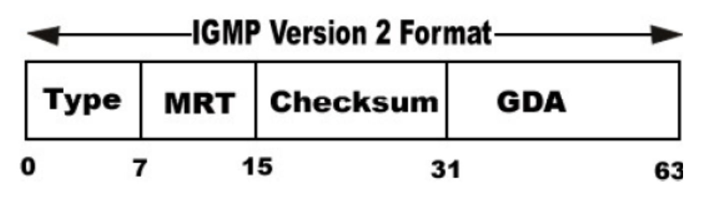


图 15-4　IGMPV2 的消息格式

类型（Type）：

0x11 = 成员关系（Membership Query）查询

有两个成员关系查询的子类型：

- 一般查询(General Query)，用于了解一个组中是否有成员在相邻的网络中。

- 特定组查询（Group-Specific Query），用于了解在相邻的网络中特定的组是否有成员。

0x16 = 版本 2 成员关系报告。

0x17 = 离开组

0x12 = 版本 1 成员报告，保证和 IGMP v1 兼容。

大响应时间（MRT，Max Response Time）：

最大的响应时间域仅在成员关系查询中有效。规定了在发送一个回应报文时最大的允许时间，(其单位为 1/10 秒)。在所有其它的消息中，会由发送者置为 0，而接收者则忽略该域。

校验字（Checksum）：

校验字是 IGMP 消息长度(IP 包的整个有效负载)的 16 位检测。该域设为 0，在计算校验字时将该域包在一起进行计算。当传送包的时候，必须计算该校验字并插入到该域中去。当接收包的时候，该校验字必须在处理该包之前进

行检验。

组地址（GDA）：

在成员关系查询消息中，发送一般查询(General Query)时组地址域应设为 0。当发送一个特定组查询（Group-Specific Query）时，则应设置组的地址。在成员报告或离开组的消息中，组的地址域设置为要报告或要离开的地址。

15.2 IGMP 协议实现

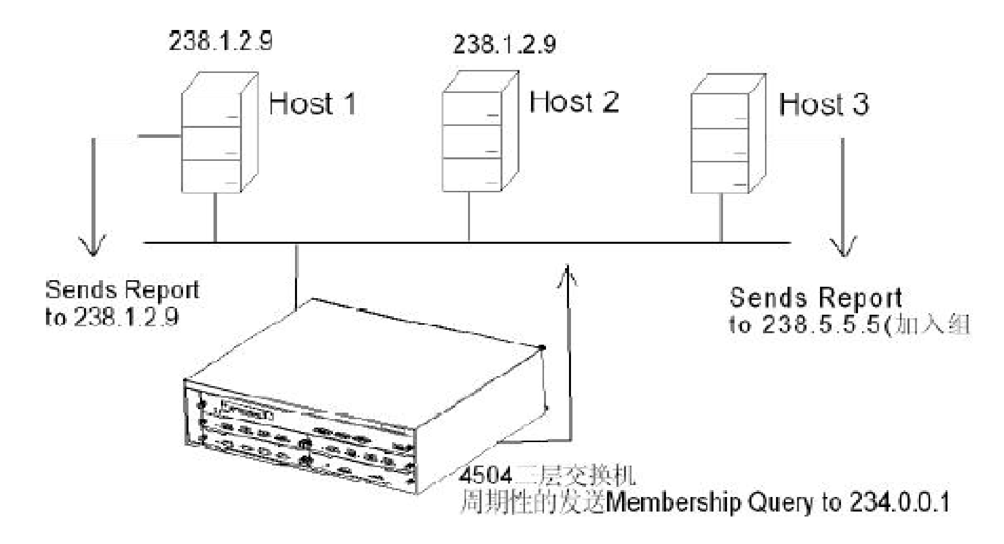


图 15-5 加入组的 IGMP 协议过程

IGMP 路由器周期性的发送 Membership Query 到 224.0.0.1（所有主机组地址），当主机接收到了一般查询，它会给每个组(有查询请求到达并且接口包含成员存在)都设一个延时定时器(Host1 和 Host2)，每一个定时器都设为一个不同的随机值，该值由主机上所能有的最高时钟频率产生。当组的定时器到时后，主机组播一个版本为 2、TTL 为 1 的成员报告到该组中（如图 5 中 Host1 发送报告）。如主机接收到了另一个主机的报告(如图中 Host2)，而其本身的定时器还没有到时，则它会停止其特定组的定时器，且不发送报告，这样就减少了重复的报告。

当主机需要加入某一特定组时，将会发送一个报告给该组（如图中 Host3）。当 IGMP 路由器接收到了报告，它就会把该组报告加入到一个组播组成员（multicast group memberships）列表中，设置组成员生存周期[Group Membership Interval]定时器。重复的报告会导致该定时器的刷新。如果在定时器到时之前没有接收到特定组报告，路由器则会假定没有本地的成员，它也不再需要在邻接的网络上为该组转发组播消息了。

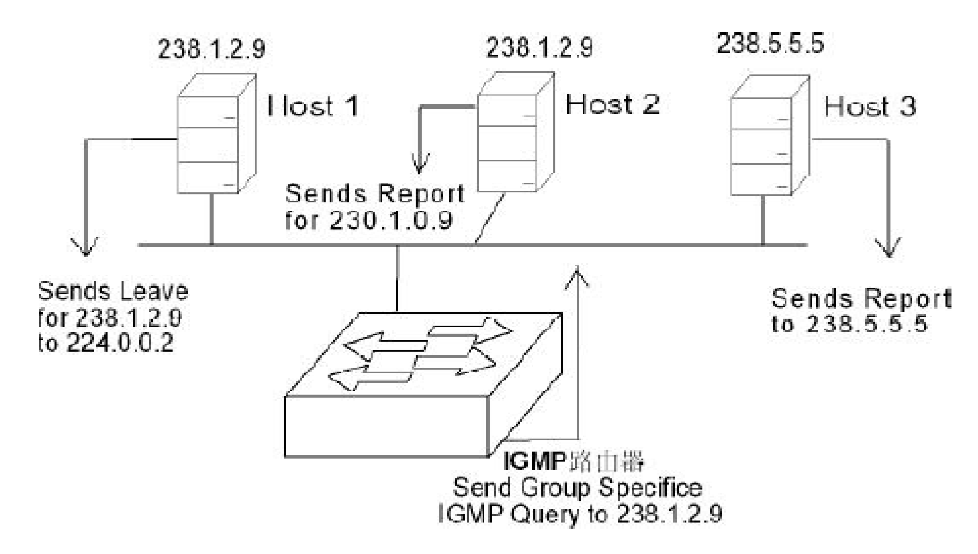


图 15-6　离开组的 IGMP 协议过程

当主机离开组播组（如图 6 中 Host1），按照 RFC2236 定义，它可以发送一条离开组的消息给 IGMP 路由器，地址为 224.0.0.2（所有 IGMP 路由器）。

当处于查询状态的 IGMP 路由器在其接口上接收到了组成员离开组的消息之后，它将在每个最后成员查询周期[Last Member Query Interval]发送最后成员查询计数[Last Member Query Count]特定组成员关系查询消息给正离开的组。这些特定组查询有最大的响应时间(设为最后成员查询周期)。如果在最后查询的响应时间之后，没有接到报告消息，路由器则会假定该组没有本地的成员。

一个主机可以加入两个不同的组，就像上图中的 Host2，Host3 由于是 238.5.5.5 组成员，所以其将周期性的发送 Report 来响应路由器一般查询。

15.3 IGMP 配置

● **用户命令：** enable igmpinterface

输入： 用户输入接口 IP 地址

功能： 使能接口对 IGMP 的支持，在交换机此接口被使能后，将周期性的发送查询报文到此接口连接的所有主机。

命令格式：

Switch# en igmp

IGMP Interface Enable

Interface IP Address(e.g. 192.168.0.1):

接口关闭命令

● **用户命令：** disable igmpinterface

输入： 用户输入接口 IP 地址

功能： 关闭接口对 IGMP 的支持，关闭后交换机将不会周期性发送查询报文。

命令格式：

Switch# dis igmp

IGMP Interface Enable

Interface IP Address(e.g. 192.168.0.1):

显示组播组命令

- **用户命令：** show igmp group

输入： 无

功能： 显示目前存在的组播组信息

命令格式：

Switch# show igmp g

IGMP Connected Group Membership

Group Address	Interface	Last Reporter	Uptime	Expires
238.1.2.9	200.1.1.1	200.1.1.20	7	350
224.0.0.9	200.1.1.1	200.1.1.1	35	350
224.0.0.9	192.168.0.1	192.168.0.1	22	350

Group Address：组播组地址

Interface：接口地址

Last Reporter：最后一个发送 report 包的源 IP 地址

Uptime：组已经存活时间，单位为秒

Expires：组生命周期，单位为秒

显示接口信息命令

- **用户命令：** show igmp interface

输入： 无

功能： 显示接口信息

命令格式：

Switch# show igmp i

Show IGMP Interface State:

Interface	Byte_In	Byte_Out	Pkt_In	Pkt_Out
200.1.1.1	900	0	15	0
192.168.0.1	0	0	0	0

Interface：接口 IP 地址

Byte_In：进入接口包大小，单位为 Byte

Byte_Out：接口送出包大小，单位为 Byte

Pkt_In：进入接口包个数

Pkt_Out：接口送出包个数

第 16 章 配置管理服务

本章描述如何配置管理服务，主要包括以下的内容：

1、管理服务介绍

2、管理服务配置

3、管理服务配置示例

在网络中，交换机本身的安全性至关重要，也是管理员非常关注的一个问题。iSpirit 3626 交换机除了提供用户名和口令来控制交换机本身的安全以外，还提供了对管理服务的控制来实现交换机的安全。

iSpirit 3626 交换机提供了 TELNET、WEB 和 SNMP 服务来实现交换机的远程管理，通过对这些服务的控制，如关闭或开启这些服务，把服务与 ACL 资源库联系起来等，来实现交换机管理的安全。

16.1 管理服务介绍

交换机管理除了串口外，还有 TELNET、WEB 和 SNMP 三种访问控制方式，后三种由于可以远程操作交换机，从而不受时间和地域限制，而备受管理员欢迎。但是随之而来的安全问题也不容忽视。特别是安全性要求高的地方，除了中心操作室的人员外，不允许外面的用户操作交换机，或者，只允许特殊的用户操作交换机，这时提供管理服务的控制的功能非常重要。

根据不同的需求，管理员可以关闭 TELNET、WEB 或（和）SNMP 服务，管理员或用户不能通过这些关闭的服务访问交换机。例如交换机关闭了 TELNET 服务，那一切试图通过 TELNET 登陆交换机的用户将不能成功。

当交换机的管理服务都被关闭时，设备可以获得很好的安全性。其实现方法主要是根据客户端和服务端通讯的原理，在服务对进入的用户管理信息进行判断，对于以上三种进入方式，判断管理员是否打开了相应的服务，如果没有打开，则用户不能使用该项服务登陆交换机。

如果管理员需要 TELNET、WEB 或（和）SNMP 服务，那需要的服务必须打开，此时拥有用户名和口令的用户可以从任何一台终端上从打开的这些服务管理交换机。这时交换机是非常不安全的，用户名和口令很容易被攻击者盗用，此时攻击者可以登陆到交换机上对设备进行破坏。

iSpirit 3626 交换机通过管理服务与 ACL 相结合的方法实现打开的管理服务的安全性。交换机使用 ACL 资源库中的标准 IP 规则组对访问进行控制，只允许从合法的 IP 地址的终端访问交换机的服务，不允许非法的 IP 地址的终端访问交换机的服务。

当交换机的管理服务是打开的，通过使用 ACL 使设备获得很好的安全性。其实现方法主要是根据客户端和服务端通讯的原理，在服务对进入的用户管理信息进行判断，对于以上三种进入方式，判断管理员是否打开了相应的服务，如果服务是打开的，判断是否设置了 ACL，如果设置了 ACL，根据 ACL 的规则对源 IP 地址进行判断，如果源 IP 地址允许访问，则可使用该项服务管理交换机，如果源 IP 地址不允许访问，则不能使用该项服务管理交换机。

在交换机的管理服务使用 ACL 之前，需要配置好 ACL 资源库中的 ACL 规则，管理服务选用 ACL 资源库中的 ACL 规则，一个管理服务只能选用一个标准 IP 规则组。

如图 15-1 是一个管理服务控制的例子，假设用户 1 和用户 2 都知道交换机管理的用户名和口令。如果 TELNET 服务是打开的，那么用户 1 和用户 2 都可以通过 TELNET 服务管理交换机。如果 WEB 服务是关闭的，那么用户 1 和

用户 2 都不可以通过 WEB 服务管理交换机。如果 SNMP 服务是打开的，但使用了 ACL 资源库中的一个标准 IP 规则组，该组规则只允许源地址为 192.168.0.100 通过，那么只有用户 1 可以通过 SNMP 服务管理交换机，用户 2 不能通过 SNMP 服务管理交换机。

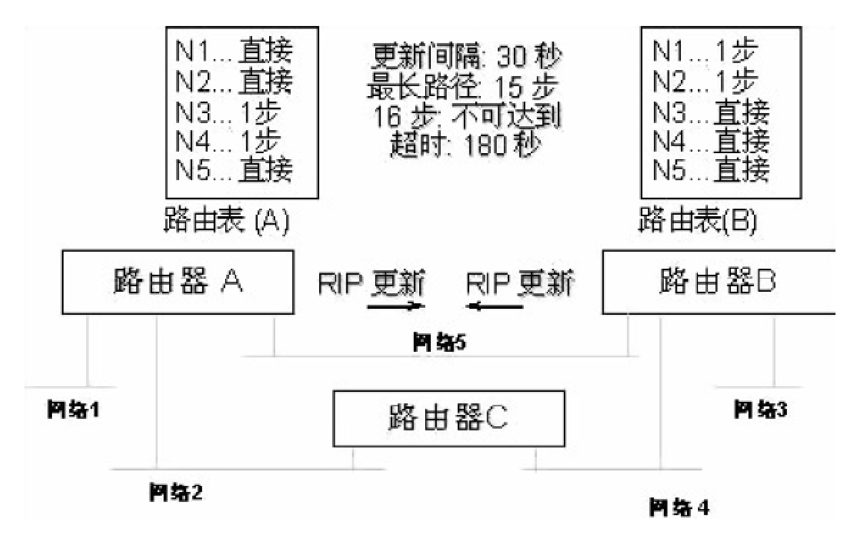


图 16-1　设备管理服务控制

16.2 管理服务配置

iSpirit 3626 交换机缺省情况下 TELNET、WEB 和 SNMP 服务都是打开的。

● 下面的命令在全局 CONFIG 模式下打开 TELNET 服务。如果不输入 group-id 参数，TELNET 服务打开但不使用 ACL 规则控制，用户可以从任何终端通过 TELNET 服务登陆交换机。如果输入 group-id 参数，TELNET 服务打开且使用 ACL 规则控制，只有 ACL 允许的 IP 地址的终端可以通过 TELNET 服务登陆交换机。group-id 的范围是从 1 到 199：

enable telnet [group-id]

● 下面的命令在全局 CONFIG 模式下关闭 TELNET 服务，此时用户不能通过 TELNET 登陆交换机：

disable telnet

● 下面的命令在全局 CONFIG 模式下配置 TELNET 的服务端口：

Switch# set telnet port <port-num>

● 下面的命令在全局 CONFIG 模式下配置 TELNET 的登录密码：

Switch# set telnet password <password>

● 下面的命令在全局 CONFIG 模式下打开 WEB 服务。如果不输入 group-id 参数，WEB 服务打开但不使用 ACL 规则控制，用户可以从任何终端通过 WEB 服务管理交换机。如果输入 group-id 参数，WEB 服务打开且使用 ACL 规则控制，只有 ACL 允许的 IP 地址的终端可以通过 WEB 服务管理交换机。group-id 的范围是从 1 到 199：

enable web [group-id]

● 下面的命令在全局 CONFIG 模式下关闭 WEB 服务，此时用户不能通过 WEB 服务管理交换机：

disable web

● 下面的命令配置在全局 CONFIG 模式 WEB 服务端口：

Switch# set web port [port-num]

- 下面的命令在全局 CONFIG 模式下打开 SNMP 服务。如果不输入 group-id 参数，SNMP 服务打开但不使用 ACL 规则控制，用户可以从任何终端通过 SNMP 服务管理交换机。如果输入 group-id 参数，SNMP 服务打开且使用 ACL 规则控制，只有 ACL 允许的 IP 地址的终端可以通过 SNMP 服务管理交换机。group-id 的范围是从 1 到 199：

  enable snmp [group-id]

- 下面的命令在全局 CONFIG 模式下关闭 SNMP 服务，此时用户不能通过 SNMP 服务管理交换机：

  disable snmp

- 下面的命令在全局 CONFIG 模式下显示 TELNET、WEB 和 SNMP 服务的配置情况：

  show manage-safety

第 17 章 配置 SNMP 和 RMON

iSpirit 3626 交换机提供了 SNMP 和 RMON 对交换机进行远程管理。本章描述如何配置 SNMP 和 RMON，主要包括以下内容：

1、SNMP 介绍

2、RMON 介绍

3、SNMP 配置

4、RMON 配置

17.1 SNMP 介绍

SNMP 是简单网络管理协议，是目前使用最广泛的网络管理协议，它具有五大功能：故障管理，计费管理，配置管理，性能管理，安全管理。它提供网管应用软件和网管代理（agent）之间通信的信息格式。

SNMP 网络管理协议有四大要素：管理工作站，管理代理，管理信息库，网络管理协议。管理代理在交换机上，是管理工作站访问交换机的服务端，管理工作站访问网管代理的信息以 MIB 的形式组织，形成管理信息库。

SNMP 有三大操作：GET 操作，SET 操作，TRAP 操作。GET 操作使管理工作站能够获取代理中对象的值。SET 操作使管理工作站能够设置代理中对象的值。TRAP 操作使代理能够想管理工作站通告重要事件。

TRAP 消息是当交换机发生事件时主动发给管理工作站的，这些消息包括冷启动，热启动，端口的 link up、link down，共用体名的认证失败，STP 的状态切换，RMON 的 EVENT 被触发的信息等。

目前 SNMP 有三个版本：SNMPV1，SNMPV2，SNMPV3 个，后面的版本是前面的升级版，功能进行了增强，安全性得到提高。iSpirit 3626 交换机支持所有的三个 SNMP 版本，可以对三个版本的 SNMP 协议包进行解析。当发送 TRAP 消息时，可以使用 SNMPV1，SNMPV2 和 SNMPV3 中的任何一个版本发送。

iSpirit 3626 交换机支持 MIB1 和 MIB2 两种 MIB 类型对象，同时支持大量的 RFC，BRIDGE 和私有的 MIB 对象，通过 SNMP 可以完全管理交换机。下面列出了 iSpirit 3626 交换机支持的一些 MIB：

RFC 1213 **RFC1213-MIB** MIB II All groups except egp and transmission.

RFC 1493 BRIDGE-MIB dot1dBase and dot1dStp groups.

RFC 1724 **RIPv2-MIB** Conformance groups 1, 2, 3.

RFC 1757 **RMON-MIB** RMON-Lite (4 RMON1 groups)1-statistics, 2-history, 3-alarm, and 9-event.

RFC 1850 **OSPF-MIB** OSPFv2 MIB. Conformance groups 1to 4 and 6 to 13 (traps are notsupported).

RFC 1907 **SNMPv2-MIB** Conformance groups 5, 6, 7, 8, 9.Also used for SNMPv3.

RFC 2233 **IF-MIB** Interface group extension for SMIv2CG= 4, 5, 6, 7, 10, 11, 13.

RFC 2571 **SNMP-FRAMEWORK-MIB** SNMPv3 MIB. SNMP ManagementFrameworks. CG=1.

RFC 2572 **SNMP-MPD-MIB** SNMPv3 MIB. SNMP Message Processing and Dispatching. CG=1.

RFC 2573 **SNMP-TARGET-MIB** SNMPv3 MIB. Define management targets. CG=1, 2, 3.

SNMP-NOTIFICATION-MIB SNMPv3 MIB. Notification generation configuration. CG=1, 2.

RFC 2574 **SNMP-USER-BASED-SM-MIB** SNMPv3 MIB. Define SNMP USM.CG=1.

RFC 2575 **SNMP-VIEW-BASED-ACM-MIB** SNMPv3 MIB. Define SNMP VACM.CG=1.

RFC 2665 EtherLike-MIB dot3StatsTable group for SMIv2.

RFC 2674 **P-BRIDGE-MIB** Conformance groups 1, 2, 3, 4, 6, 8, 9. **Q-BRIDGE-MIB** Conformance groups 1, 3, 4, ½ of 5, 6,7, 8.

如图 16-1 是管理工作站与管理代理之间的 SNMP 协议交互的例子。管理工作站可以通过发送 Get Request、Get_next Request 和 Set Request 的 SNMP 消息访问交换机管理代理，获取或设置交换机的 MIB 对象的值，交换机管理代理回送 Get Response 的 SNMP 消息给管理工作站。当交换机上发生了一些事件时，交换机的管理代理主动发送 SNMP TRAP 消息给管理工作站。

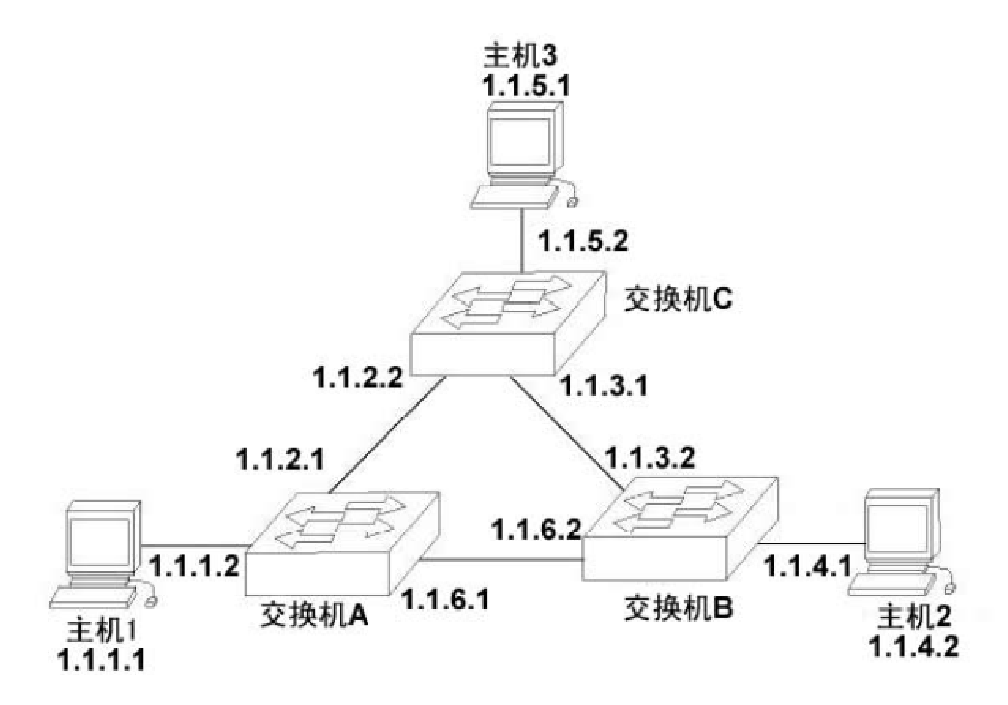


图 17-1　管理工作站和管理代理之间的 SNMP 协议交互

17.2 RMON 介绍

RMON(Remote Network Monitoring，远程网络监测)作用于定义标准的网络监视功能和接口，使基于 SNMP 的管理终端和远程监视器之间能够通信。RMON 提供了两种控制特征：配置和操作调用。

1.配置

远程监测器需要为数据采集进行配置。配置指定要采集的数据类型和形式。RMON MIB 被分成一定数量的功能组，在每一组内部，有一个或多个控制表和一个或多个资料表。控制表是典型可以读写的表，包含资料表中的资料参数，而资料表是只读的。这样，在配置时，管理终端设定合适的配置参数来配置远程监视器来采集想要的数据。

2.操作调用

操作调用是 SNMP 通过 set 操作来发送一个命令。

RMON 表管理的操作包括：添加、删除，修改和读取。RMON 在进行表操作时都要涉及到行字段操作。在 statistics 组中的 etherStatsStatus，history 组中的 historyControlStatus，alarm 组中的 alarmStatus 和 event 组中的 eventStatus。

他们的取值都是 valid(1), createRequest(2),

UnderCreation(3)和 invalid(4)。

添加：在添加行时先对行字段作 createRequest（2）操作，完成操作后行字段状态自动迁移到 underCreation（3）；当配置完其它的有效字段操作后，再对行字段作 valid（1）操作，行字段变为 valid（1）。

修改：当要修改表项时，需要先配置行字段为 underCreation（3），再修改其它字段，修改完后,对行字段作 valid（1）操作，行字段变为 valid（1）。在行字段为 valid（1）状态下，不能修改其它字段。

删除：配置行字段状态为 invalid（4）就可以删除一行。

iSpirit 3626 交换机支持 1、2、3、9 组 RMON MIB，分别是 statistics 组，history 组，alarm 组和 event 组。

17.3 SNMP 配置

SNMP 配置包括交换机的 community 配置和 TRAP 工作站的配置。iSpirit 3626 交换机缺省有一个只读的共用体，共用体名为 public，交换机最多可以配置 8 个共用体。iSpirit 3626 交换机缺省没有配置 TRAP 工作站，交换机最多可以配置 8 个 TRAP 工作站。

SNMP 的命令如下：

- snmp community

模式：CONFIGURATION

参数：参数以交互式输入

Community Name：共用体名称

Permission：读写权限，1)只读，2)读写

功能：配置访问网管的共用体名称，这是一个交互式命令。配置时用户可以根据提示输入需要的创建的共用体名称，和读/写权限。

- snmp trap

模式：CONFIGURATION

参数：参数以交互式输入

trap name：trap 名称

Target Ip Addr：Trap 发送的目标 IP 地址

Version：Trap 发送的版本 v1，v2，v3

功能：添加或修改 snmp trap 的发送目标。这是一个交互式命令。Trap name 是唯一的，如果修改了已经存在的 name，则可以修改这个 trap 发送目标项。Target ip addr 是发送 trap 的目标地址；version 是以 snmpV1，snmpV2 还是 snmpV3 的方式发送。这个命令缺省配置了目标端口是 162。

- show snmp trap

模式：CONFIGURATION

功能：显示所有的 trap 配置。

- no snmp trap <trap-name>

模式：CONFIGURATION

功能：删除指定 name 的 trap 项。

- snmp trap ip <trap-name> <ip-address>

模式：CONFIGURATION

参数：

trap-name：Trap 名称

ip-address：目标 IP 地址

功能：修改指定 trap-name 的目的 ip 地址为 ip-address

● snmp trap port <trap-name> <port>

模式：CONFIGURATION

参数：

trap-name：Trap 名称

port：目标端口

功能：修改指定 trap-name 的目的 port。

● snmp trap retries <trap-name> <retries>

模式：CONFIGURATION

参数：

trap-name：trap 名称

retries：重发次数

功能：修改指定 trap-name 的 trap 项的重发次数为 retries 次。SnmpV1 不支持这个参数。

● snmp trap timeout<trap-name> <timeout>

模式：CONFIGURATION

参数：

trap-name：Trap 名称

retries：超时时间

功能：修改指定 trap-name 的 trap 项的发送超时为 timeout，timeout 的单位是 1/100 秒，SnmpV1 不支持这个参数。由于 udp 没有确认机制，所以配置了 retries 和 timeout 时，每条 trap 会间隔 timeout/100 秒发送 retries 次。

● snmp trap version <trap-name><version>

模式：CONFIGURATION

参数：

Trap-name：Trap 名称

Retries：超时时间

功能：修改指定 trap-name 的 trap 项的发送版本。

17.4 RMON 配置

RMON 的命令如下：

● rmon statistics [index]

模式：CONFIGURATION

参数：

index：索引，Index 是可选项，如果没有输入系统缺省生成一个 index 值。

功能：配置 statistics 组的被监视端口的基本统计数据。每一行对应一个被监视的接口。iSpirit 3626 缺省配置了

12 项。交互式输入中 etherStatsDataSource 指被监视端口的接口索引的 objectId。

● rmon alarm [index]

模式：CONFIGURATION

参数：

index：索引，Index 是可选项，如果没有输入系统缺省生成一个 index 值。

rmon alarm 命令是一个交互式命令，如果输入了 index 则添加或修改指定的组。下面介绍 alarm 交互式输入字段：

Interval：间隔取值时间，单位为秒。（建议取值 2 秒）

Variable：被监视的节点。类型必须是 INTEGER (INTEGER, Counter, Gauge,or TimeTicks)

SampleType：计算要与阀值比较的数值的方法。如果该对象的取值为 absoluteValue (1)，则所选变量的取值直接和阀值相比较。如果该对象的取值为 deltaValue(2)，则在所选变量的上一个采用的取值减去当前值后，起差值于阀值相比较。

StartupAlarm：取值为 risingAlarm(1), fallingAlarm(2), risingOrFallingAlarm(3)。指定在一行有效后，risingThreshold 时第一个取样大于活等于，fallingThreshold 时小于或等于，或者两者都是时是否产生警告。

RisingThreshold：取样统计的上限阀值。

RisingEventIndex：当超过上限时所用的 eventEntry 索引。

FallingThreshold：取样统计的下限阀值。

FallingEventIndex：当超过下限时所用的 eventEntry 索引。

功能：alarm 组用来定义网络性能的一系列阀值。如果阀值在某一方面被超过以后，就会产生警告。Alarm 组由一个表 alarmtable 组成。表中的每一条目都规定了要监视的特定变量，取样时间间隔和阀值参数。

● rmon event [index]

模式：CONFIGURATION

参数：

index：索引，Index 是可选项，如果没有输入系统缺省生成一个 index 值。

功能：event 组支持事件定义。事件由 MIB 其它地方的条件所引发，时间也能引发定义在 MIB 其它地方的动作。事件可能导致该组中记录信息，或是发出 SNMP Trap 消息。

rmon event 命令是一个交互式命令，如果输入了 index 则添加或修改指定的组。下面介绍 event 交互式输入字段中 EventType：事件类型，none(1)，log(2)，snmp-trap(3)，log-and-trap(4)。

● no rmon alarm <index>

模式：CONFIGURATION

参数：

index：索引。

功能：删除指定索引 index 的 alarm 配置 entry 项。

● no rmon event <index>

模式：CONFIGURATION

参数：

index：索引。

功能：删除指定索引 index 的 event 配置 entry 项。

- no rmon statistics <index>

模式：CONFIGURATION

参数：

index：索引。

功能：删除指定索引 index 的 statistics 配置 entry 项。

- show rmon configuration alarm [index]

模式：CONFIGURATION

参数：

index：索引。

功能：显示 alarm 的配置表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

show rmon configuration even [index]

模式：CONFIGURATION

参数：

index：索引。

功能：显示 event 的配置表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

- show rmon table even [index]

模式：CONFIGURATION

参数：

index：索引。

功能：显示 event 的资料表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

- show rmon table statistics [index]

模式：CONFIGURATION

参数：

index：索引。

功能：显示 statistics 的资料表，如果输入了 index 则显示指定 index 的配置项，否则显示全部配置项。

第 18 章 配置调试工具

在实际应用中，网络经常会出现一些故障或问题，需要有一些工具来对问题进行跟踪和定位。iSpirit 3626 交换机提供了多种调试工具，可对交换机本身或网络中的一些问题进行跟踪和定位。

本章对这些调试工具的使用和配置进行详细的描述，主要包括以下内容：

1、调试工具介绍

2、调试工具配置

3、调试工具配置示例

18.1 调试工具介绍

iSpirit 3626 交换机提供了多种调试工具，主要有：IP DEBUG 工具、PING 工具、TRACEROUTE 工具和 TELNET 客户端工具。

本节对这些调试工具进行详细的描述，主要包括以下内容：

- IP DEBUG 工具介绍
- PING 工具介绍
- TRACEROUTE 工具介绍
- TELNET 客户端工具介绍

1. IP DEBUG工具介绍

IP DEBUG 工具的个用途是在终端上显示交换机收发的数据流的基本信息，如可以抓取收发的 ARP 数据流的基本信息。

通过在终端上配置相应的命令，如果有相应的事件发生或数据流收发时，可以在终端上显示这些信息，便于调试和诊断交换机和网络中的故障和问题。

通过这些 IP DEBUG 命令管理员可以确认交换机是否收到或者发出具体的协议包，可以在终端上显示一些相应的信息，如对于 TCP 协议包，可以显示 TCP 目的端口和源端口等。

iSpirit 3626 交换机支持一个串口终端和 5 个 TELNET 终端。这些终端上都可以配置 IP DEBUG 命令。当一个终端上打开了 DEBUG 配置后，只针对这个终端，相应的调试信息也只显示在这个终端上，不会影响其它的终端。如一个终端 A 上打开了 ARP DEBUG，另一个终端 B 打开了 TCP DEBUG，那么 ARP 的调试信息会显示在终端 A 终端上，TCP 的调试信息会显示在 B 终端上。如果两个或多个终端打开了相同的 DEBUG 配置，则相应的调试信息会显示在所有的打开配置的终端上。如一个终端 A 和另一个终端 B 上打开了 ARP DEBUG 配置，那么 ARP 调试信息会显示在终端 A 和 B 上。

当在终端上打开 DEBUG 配置时，交换机的系统的性能会有一定的影响，特别是收发包的性能会受到影响。所以建议用户只有在需要对交换机或网络进行调试诊断时才打开 DEBUG 配置，当完成时关闭所有的 DEBUG 配置。

因为 TELNET 终端本身需要 PC 机与交换机进行 TELNET 通信，所以在 TELNET 上不能打开 IP 和 TCP 的 DEBUG 配置，否则会出现一个数据流抓取的死循环，耗尽系统的所有资源。

2. PING工具介绍

iSpirit 3626 交换机提供了一个 PING 工具，用于检测交换机到目的设备的连通性。PING 工具使用 ICMP 协议，当交换机 PING 一个目的设备时，交换机首先发出一个 ICMP 回送请求包，等待一个匹配的 ICMP 回送应答包，如果收到表明交换机到目的设备是连通的，如果在规定的时间内没有收到 ICMP 回送应答包，交换机重发 ICMP 回送请求包，如果在规定的次数内没有收到 ICMP 回送应答包，则表明交换机到目的设备不通。

iSpirit 3626 交换机提供了一个简单的 PING 命令和一个复杂的 PING 命令。简单的 PING 命令只是检测交换机到目的设备的连通性，交换机一共发 5 个 ICMP 回送请求包，看接收到的 ICMP 回送应答包的情况。复杂的 PING 命令除了可以检测交换机到目的设备的连通性，还有以下的功能：

可以指定发送的 ICMP 回送请求包的个数。

可以指定发送 ICMP 回送请求包后等待的超时时间间隔。

可以指定发送的 ICMP 回送请求包的数据区大小。

可以指定发送的 ICMP 回送请求包的源地址。

可以指定发送的 ICMP 回送请求包中带记录路由，可以记录交换机到目的设备中经过的设备地址。

可以指定发送的 ICMP 回送请求包中带不严格的源站路由，可以按照指定的路径检测交换机到目的设备之间的连通性。

可以指定发送的 ICMP 回送请求包中带严格的源站路由，可以按照指定的路径检测交换机到目的设备之间的连通性。

可以指定发送的 ICMP 回送请求包中带时间戳记录路由，可以记录交换机到目的设备中经过的设备地址和时间戳。

3. TRACEROUTE工具介绍

iSpirit 3626 交换机提供一个 TRACEROUTE 工具，可以发现交换机到目的设备经过的每一个路由设备，可以确定交换机到目的设备之间的路径，如果交换机到目的设备不通，可以精确定位到是因为中间哪个设备的问题。

iSpirit 3626 交换机的 TRACEROUTE 工具使用 UDP 协议包进行探测，交换机发 TTL 依次递增的 UDP 包，通过接收返回的 ICMP 错误包来检测状态，直到交换机发现了 UDP 目的端口不可达的 ICMP 包。在交换机上会显示交换机到每一个中间设备的状态信息，通过这些状态信息可以定位网络的问题。

iSpirit 3626 提供了一个简单的 TRACEROUTE 命令和一个复杂的 TRACEROUTE 命令。简单的 TRACEROUTE 命令只探测到目的地的中间设备的情况，复杂的 TRACEROUTE 命令还有以下的功能：

可以指定发送的 UDP 包的源地址。

可以指定发送 UDP 包后的超时时间间隔。

可以指定每个中间设备探测的次数。

可以指定最小和最大的 TTL。

可以指定 UDP 目的端口号。

可以指定发送的 UDP 包带记录路由，可以记录交换机到目的设备中经过的设备地址。

可以指定发送的 UDP 包中带不严格的源站路由，可以按照指定的路径检测交换机到目的设备之间的连通性。

可以指定发送的 UDP 包中带严格的源站路由，可以按照指定的路径检测交换机到目的设备之间的连通性。

可以指定发送的 UDP 包中带时间戳记录路由，可以记录交换机到目的设备中经过的设备地址和时间戳。

4.TELNET客户端工具介绍

iSpirit 3626 交换机提供一个 TELNET 客户端工具，可以从交换机上 TELNET 到另一个设备上，对设备进行配置

和管理。

iSpirit 3626 交换机有一个串口终端和 5 个 TELNET 终端，从串口终端或 TELNET 终端上可以执行 TELNET 命令登陆到目的设备，对目的设备进行管理。iSpirit 3626 交换机只支持一个 TELNET 客户端，当 TELNET 客户端已被一个终端使用时，另外的终端不能使用 TELNET 客户端，必须等到使用 TELNET 客户端的终端退出时才能使用 TELNET 客户端。

18.2 调试工具配置

本节介绍如何配置调试工具，主要包括以下内容：

- IP DEBUG 工具配置
- PING 工具配置
- TRACEROUTE 工具配置
- TELNET 客户端工具配置

1. IP DEBUG工具配置

iSpirit 3626 交换机缺省情况下所有的 1 个串口终端和 5 个 TELNET 终端上的 DEBUG 配置都是关闭的。

- 下面的命令在全局 CONFIG 模式下打开 IP 的 DEBUG 配置：

  debug ip

- 下面的命令在全局 CONFIG 模式下关闭 IP 的 DEBUG 配置：

  no debug ip

  注意：

  上面的两个命令只能在串口终端上使用，不能在 TELNET 终端上使用。

- 下面的命令在全局 CONFIG 模式下打开 ARP 的 DEBUG 配置：

  debug ip arp

- 下面的命令在全局 CONFIG 模式下关闭 ARP 的 DEBUG 配置：

  no debug ip arp

- 下面的命令在全局 CONFIG 模式下打开 TCP 的 DEBUG 配置：

  debug ip tcp

- 下面的命令在全局 CONFIG 模式下关闭 TCP 的 DEBUG 配置：

  no debug ip tcp

  注意：

  上面的两个命令只能在串口终端上使用，不能在 TELNET 终端上使用。

- 下面的命令在全局 CONFIG 模式下打开 UDP 的 DEBUG 配置：

  debug ip udp

- 下面的命令在全局 CONFIG 模式下关闭 UDP 的 DEBUG 配置：

  no debug ip udp

- 下面的命令在全局 CONFIG 模式下打开 ICMP 的 DEBUG 配置：

debug ip icmp

● 下面的命令在全局 CONFIG 模式下关闭 ICMP 的 DEBUG 配置：

no debug ip icmp

● 下面的命令在全局 CONFIG 模式下打开 SNMP 的 DEBUG 配置：

debug ip snmp

● 下面的命令在全局 CONFIG 模式下关闭 SNMP 的 DEBUG 配置：

no debug ip snmp

● 下面的命令在全局 CONFIG 模式下打开 IGMP 的 DEBUG 配置：

debug ip igmp

● 下面的命令在全局 CONFIG 模式下关闭 IGMP 的 DEBUG 配置：

no debug ip igmp

● 下面的命令在全局 CONFIG 模式下打开 IGMP SNOOPING 的 DEBUG 配置：

debug ip igmpsnooping

● 下面的命令在全局 CONFIG 模式下关闭 IGMP SNOOPING 的 DEBUG 配置：

no debug ip igmpsnooping

● 下面的命令在全局 CONFIG 模式下关闭所有的 DEBUG 配置：

no debug all

● 下面的命令在全局 CONFIG 模式下显示 DEBUG 配置信息，只把打开的 DEBUG 配置显示出来：

show ip debug-on

2.PING工具配置

iSpirit 3626 交换机提供了一个简单和一个复杂的 PING 命令。1 个串口终端和 5 个 TELNET 终端上都可以执行 PING 命令检测交换机到目的设备之间的连通性。

● 下面的命令在 EXEC 模式和全局 CONFIG 模式下执行，是简单的 PING 命令，可以检测交换机到目的设备之间的连通性：

ping <ip-address>

● 下面的命令在 EXEC 模式和全局 CONFIG 模式下执行，是复杂的 PING 命令。它是一个交互式命令，除了可以检测交换机到目的设备之间的连通性以外，还可以通过交互式输入不同的配置执行不同的功能：

ping

根据交互式的提示输入相应的配置。

3.TRACEROUTE工具配置

iSpirit 3626 交换机提供了一个简单和一个复杂的 TRACEROUTE 命令。1 个串口终端和 5 个 TELNET 终端上都可以执行 TRACEROUTE 命令来探测到目的地的中间设备状态。

● 下面的命令在全局 CONFIG 模式下执行，是简单的 TRACEROUTE 命令，可以探测到目的地的中间设备状态：

traceroute <ip-address>

● 下面的命令在全局 CONFIG 模式下执行，是复杂的 TRACEROUTE 命令。它是一个交互式命令，除了可以探测到目的地的中间设备状态以外，还可以通过交互式输入不同的配置执行不同的功能：

traceroute

根据交互式的提示输入相应的配置。

4.TELNET客户端工具配置

iSpirit 3626 交换机提供了一个 TELNET 命令，从 1 个串口终端或 5 个 TELNET 终端上可以执行 TELNET 命令登陆到目的设备，但 TELNET 客户端同时只能被一个终端使用。

下面的命令在全局 CONFIG 模式下登陆到目的设备：

telnet <ip-address>